



GUIDANCE NOTES

For

AML/ATF REGULATED FINANCIAL INSTITUTIONS

On

Anti-Money Laundering & Anti-Terrorist Financing (AML/ATF)

**Issued by the
Bermuda Monetary Authority**

*Pursuant to Proceeds of Crime Regulations (Supervision & Enforcement) Act 2008 (Section 5(2))
Section 49A of the Proceeds of Crime Act 1997 and Section 12B of the Anti-Terrorism (Financial and Other Measures) Act 2004*

March 2009

Contents

Preface		
CHAPTER 1		
General Institution and Senior Management Responsibilities	Page	Paragraph
Introduction	10	1.1 – 1.4
International pressure to have risk-based AML/ATF procedures	10	1.5 – 1.9
Key elements of Bermuda’s legal & regulatory AML/ATF framework	10	1.10 – 1.14
General legal and regulatory obligations	12	1.15 – 1.18
Formal policy on the prevention & detection of money laundering and terrorist financing	12	1.19 – 1.32
Application of group policies outside Bermuda	14	1.33 – 1.36
Criminal and Civil Penalties	14	1.37 – 1.40
US Patriot Act – Extra Territoriality	15	1.41
CHAPTER 2		
Internal Controls		
General legal and regulatory obligations	16	2.1 – 2.2
Appropriate controls in the context of financial crime prevention	16	2.3 – 2.5
Outsourcing and non-Bermuda processing	17	2.6 – 2.10
CHAPTER 3		
Reporting Officer		
General legal and regulatory obligations	19	3.1 – 3.5
Internal and external reports	20	3.6 – 3.12
National and international findings in respect of countries & jurisdictions	20	3.13 – 3.14
Monitoring effectiveness of money laundering controls	21	3.15
Reporting to senior management	21	3.16 – 3.22
CHAPTER 4		
Risk-Based Approach		
Introduction	22	4.1 – 4.5
A risk-based approach	23	4.6 – 4.12
Identifying and assessing the risks faced by the AML/ATF regulated financial institution	24	4.13 – 4.18
Designing and implementing controls to manage and mitigate the risks	25	4.19 – 4.27
Monitoring and improving the effective operation of the AML/ATF regulated financial institution’s controls	26	4.28
Recording appropriately what has been done and why	27	4.29
Risk management is dynamic	27	4.30 – 4.34
CHAPTER 5		
Customer Due Diligence		
Meaning of customer due diligence measures and on-going monitoring	28	5.1 – 5.4
What is customer due diligence?	29	5.5 – 5.8
What is on-going monitoring?	29	5.9
Why is it necessary to apply CDD measures and on-going monitoring?	30	5.10 – 5.13
Other material, pointing to good practice	30	5.14
Timing of, and non compliance with, CDD measures	30	5.15
Timing of verification	31	5.16 – 5.19
Requirement to cease transactions, etc.	31	5.20 – 5.23
Application of CDD measures	32	5.24
Identification and verification of the customer	32	5.25 – 5.30
Identification and verification of a beneficial owner	32	5.31 – 5.36
Customers with whom AML/ATF regulated institutions have a business relationship on 1 st January 2009	33	5.37 – 5.40
Acquisition of one AML/ATF regulated financial institution, or a portfolio of customers, by another	34	5.41 – 5.42
Nature and purpose of proposed business relationship	34	5.43 – 5.44
Keeping information up to date	34	5.45
Characteristics and evidence of identity	35	5.46 – 5.50

Documentary evidence	35	5.51 – 5.53
Electronic evidence	36	5.54 – 5.55
Nature of electronic checks	36	5.56 – 5.59
Criteria for use of an electronic data provider	36	5.60 – 5.61
Shell banks and anonymous accounts	36	5.62 – 5.64
Private individuals	37	5.65 – 5.78
Electronic verification	38	5.79 – 5.82
Mitigation of impersonation risk	39	5.83
Variation from standard	39	5.84 – 5.86
Executors and personal representatives	40	5.87 – 5.88
Attorneys	40	5.89 – 5.91
Source of funds as evidence	40	5.92 – 5.96
Customers who cannot provide the standard evidence	41	5.97 – 5.101
Students and young people	41	5.102 – 5.103
Customers other than private individuals	41	5.104 – 5.108
Corporates	42	5.109 – 5.119
Companies listed on an appointed stock exchange	43	5.120 – 5.122
Private and unlisted companies	44	5.123 – 5.135
Pension schemes	45	5.136 – 5.142
Charities, church bodies and places of worship	46	5.143 – 5.152
Registered charities	47	5.153
Independent schools and colleges	47	5.154 – 5.159
Other trusts, foundations and similar entities	48	5.160 – 5.182
Other entities that are subject to the Regulations (or equivalent)	50	5.183 – 5.186
Partnerships and unincorporated businesses	51	5.187 – 5.199
Clubs and societies	52	5.200 – 5.208
Simplified due diligence	53	5.209 – 5.215
Enhanced due diligence	55	5.216 – 5.223
Non face-to-face identification and verification	55	5.224 – 5.230
Politically Exposed Persons	56	5.231 – 5.244
Multipartite relationships, including reliance on third parties	58	5.245 – 5.264
Group introductions	61	5.265 – 5.268
Use of pro forma confirmations	62	5.269 – 5.272
Situations which are not reliance	62	5.273 – 5.282
Monitoring customer activity	63	5.283 – 5.303
Persons institutions should not accept as customers	66	5.304 – 5.312
CHAPTER 5		
Confirmation of Verification of Identity		
Private individual introduced by a Bermuda AML/ATF regulated financial institution	68	Annex 5-I
Private individual introduced by an AML/ATF regulated financial institution located outside Bermuda	69	Annex 5-II
Corporate & other non-personal entity introduced by a Bermuda AML/ATF regulated financial institution	70	Annex 5-III
Corporate & other non-personal entity introduced by an AML/ATF regulated financial institution located outside Bermuda	71	Annex 5-IV
Group introduction – private individual	72	Annex 5-V
Group introduction - corporate & other non-personal entity	73	Annex 5-VI
CHAPTER 6		
Suspicious Activity Reporting		
General legal and regulatory obligations	74	6.1 – 6.4
What is meant by ‘knowledge’ and ‘suspicion’?	75	6.5 – 6.9
Internal reporting	76	6.10 – 6.16
Non-Bermuda offences	76	6.17 – 6.18
Evaluation and determination by the reporting officer	77	6.19 – 6.22

External reporting	77	6.23 – 6.26
Where to report	78	6.27 – 6.28
Attempted fraud and attempted money laundering	78	6.29
Penalties	78	6.30
Consent	78	6.31
Consent under Proceeds of Crime Act 1997	78	6.32 – 6.34
Consent under Anti-Terrorism (Financial and Other Measures) Act 2004	79	6.35
Tipping Off	79	6.36 – 6.41
Transactions following a disclosure	80	6.42 – 6.45
Constructive trusts	80	6.46 – 6.51
Additional Reporting Obligations on Relevant Institutions	81	6.52
CHAPTER 7		
Staff Awareness, Training and Alertness		
Why focus on staff awareness and training?	82	7.1 – 7.4
General legal and regulatory obligations	83	7.5 – 7.7
Responsibilities of senior management	83	7.8 – 7.11
Responsibilities of staff	83	7.12 – 7.13
Legal obligations on staff	84	7.14 – 7.16
Training in the AML/ATF regulated financial institution's procedures	84	7.17 – 7.19
Staff alertness to specific situations	84	7.20 – 7.28
Staff based in a country or territory other than Bermuda	86	7.29
Training methods and assessment	86	7.30 – 7.33
CHAPTER 8		
Record Keeping		
General legal and regulatory obligations	87	8.1 – 8.4
What records have to be kept?	87	8.5 – 8.6
Customer information	88	8.7 – 8.13
Transactions	88	8.14 – 8.15
Internal and external reports	89	8.16 – 8.18
Other records	89	8.19 – 8.20
Form in which records have to be kept	89	8.21 – 8.23
Location	90	8.24 – 8.28
APPENDICES		
Appendix I – Glossary of Abbreviations and Terms	91	
Appendix II – AML/ATF Responsibilities in Bermuda	96	
Appendix III – Summary of Bermuda Legislation	98	
▪ Proceeds of Crime Act 1997	98	
▪ Anti-Terrorism (Financial and Other Measures) Act 2004	99	
▪ Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing) Regulations 2008	99	
▪ Proceeds of Crime Regulations (Supervision and Enforcement) Act 2008	100	
▪ Financial Intelligence Agency Act 2007	100	
▪ The Terrorism (United Nations Measures) (Overseas Territories) Order 2001	100	
▪ The Al-Qa'ida and Taliban (United Nations Measures) (Overseas Territories) Order 2002	100	
▪ The Al-Qa'ida and Taliban (United Nations Measures) (Overseas Territories) (Amendment) Order 2002	100	

PREFACE

1. In Bermuda, there have been long-standing obligations to have effective procedures in place to detect and prevent money laundering. The offence of money laundering has been contained in the Proceeds of Crime Act (POCA) since 1997 and obligations to combat terrorist financing set out in The Anti-Terrorism (Financial and Other Measures) Act (ATFA) since 2004. The original obligations on Regulated Institutions were established in the Proceeds of Crime (Money Laundering) Regulations, in 1998 which were supported by the Guidance Notes issued in January 1998. The Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing) Regulations 2008 (the Regulations), which came into effect on the 1st January 2009, repealed the 1998 regulations and institutions subject to the regulations are now termed “AML/ATF regulated financial institutions”.
2. Following the International Monetary Fund Review in mid 2007, a number of legislative initiatives have been finalized and passed by the Legislature. Among other things, these initiatives, which are set out in more detail in the pages following, expand the obligations on AML/ATF regulated financial institutions (“institutions”) affected by the legislation and increase the scope of the regulated sector.
3. The legislation also establishes a new regulatory regime. The Proceeds of Crime Regulations (Supervision and Enforcement) Act 2008 (SEA) designated the BMA as the supervisory body for securing compliance with the Regulations by AML/ATF regulated financial institutions (“institutions”) and also details the obligations and powers related to this duty. A new agency, the Financial Intelligence Agency, having the responsibility for the receipt and analysis of Suspicious Activity Reports commenced operations on the 15th November 2008 following the commencement of the Financial Intelligence Agency Act 2007.

Purpose of the guidance

4. The purpose of this guidance is to:
 - Outline the legal and regulatory framework for AML/ATF requirements and systems for Bermuda’s institutions;
 - Interpret the requirements of the relevant law and regulations, and how they may be implemented in practice;
 - Indicate good industry practice in AML/ATF procedures through a proportionate, risk-based approach; and
 - Assist institutions to design and implement the systems and controls necessary to mitigate the risks of the institution being used in connection with money laundering and the financing of terrorism.

Scope of the guidance

5. This guidance sets out what is expected of institutions and their staff in relation to the prevention of money laundering and terrorist financing, but allows them some discretion as to how they apply the requirements of Bermuda’s AML/ATF regime in the particular circumstances of the institution, and its products, services, transactions and customers.
6. This guidance relates solely to how institutions should fulfill their obligations under the AML/ATF law and regulations. It is important that customers understand that production of the required evidence of identity does not automatically qualify them for access to the product or service they may be seeking; institutions bring to bear other commercial considerations in deciding whether particular customers should be taken on.

What is the offence of money laundering?

7. Money laundering takes many forms, including:
 - Trying to turn money raised through criminal activity into ‘clean’ money (that is, classic money laundering);

- Being directly involved with any criminal or terrorist property, or entering into arrangements to facilitate the laundering of criminal or terrorist property; and
 - Criminals investing the proceeds of their crimes in the whole range of financial products.
8. The techniques used by money launderers constantly evolve to match the source and amount of funds to be laundered, and the legislative/regulatory/law enforcement environment of the market in which the money launderer wishes to operate. More information on the ways in which particular financial services businesses, products, relationships and technologies may be used by money launderers and terrorist financiers, along with some case study examples, is available at <http://www.fatf-gafi.org>
9. There are three broad groups of offences related to money laundering that institutions need to avoid committing. These are:
- Knowingly assisting (in a number of specified ways) in concealing, or entering into arrangements for the acquisition, use, and/or possession of the proceeds of criminal conduct;
 - Failing to report a knowledge or suspicion that another person is engaged in money laundering; and
 - ‘Tipping off’ i.e. intending to prejudice an investigation knowing or suspecting that a disclosure has been made to the Financial Intelligence Agency or that the police are acting or proposing to act in connection with an investigation into money laundering.
10. It is also a separate offence under the Regulations not to establish adequate and appropriate policies and procedures to forestall and prevent money laundering (regardless of whether or not money laundering actually takes place).

The guidance also covers terrorist financing

11. There can be considerable similarities between the movement of terrorist property and the laundering of criminal property: some terrorist groups are known to have well established links with organised criminal activity. However, there are two major differences between terrorist property and criminal property more generally:
- Often only small amounts are required to commit individual terrorist acts, thus increasing the difficulty of tracking the terrorist property; and
 - Terrorists can be funded from legitimately obtained income, including charitable donations, and it is extremely difficult to identify the stage at which legitimate funds become terrorist property.
12. Terrorist organisations can, however, require quite significant funding and property to resource their infrastructure. They often control property and funds from a variety of sources and employ modern techniques to manage these funds, and to move them between jurisdictions.
13. In combating terrorist financing, the obligations on institutions are the same as those specified for money laundering viz. reporting suspicious activity, knowingly assisting in terrorist financing, tipping off and having appropriate procedures/policies in place to combat such activities.

What about other financial crime?

14. Money laundering and terrorist financing risks are closely related to the risks of other financial crime, such as fraud. Fraud and market manipulation, as separate offences, are not dealt with in this guidance. The guidance does, however, apply to dealing with any proceeds of crime that arise from these activities.
15. Institutions increasingly look at fraud and money laundering as part of an overall strategy to tackle financial crime, and there are many similarities – as well as differences - between procedures to tackle the two. When considering money laundering and terrorist financing issues, institutions should consider their procedures against fraud and market manipulation and how these might reinforce each other. Where responsibilities are given to different departments, there will need to be strong links between those in the

institution responsible for managing and reporting on these various areas of risk. When measures involving the public are taken specifically as an anti-fraud measure, the distinction should be made clear.

Who is the guidance addressed to?

16. This guidance, which has been approved by the Minister of Justice, is issued by the Bermuda Monetary Authority under section 5(2) of the Proceeds of Crime Regulations (Supervision and Enforcement) Act 2008, section 49A of the Proceeds of Crime Act 1997 and section 12B of the Anti-Terrorism (Financial and Other Measures) Act 2004. This guidance is addressed to AML/ATF regulated financial institutions within the meaning of section 2(1) of the SEA Act. When provisions of the Regulations or the various Acts are directly described in the text of the guidance these provisions **must** be complied as they are mandatory. In other cases, the guidance uses the term **should** to indicate ways in which the requirements of the Regulations or Acts may be satisfied, but allowing for alternative means of meeting the requirements.
17. The guidance will be of direct relevance to senior management and reporting officers in institutions. The purpose is to give guidance to those who set the institution's risk management policies and its procedures for preventing money laundering and terrorist financing. Although the guidance will be relevant to operational areas, it is expected that these areas will be guided by the institution's own, often more detailed and more specific, internal arrangements, tailored by senior management to reflect the risk profile of the institution.

How should the guidance be used?

18. The guidance gives institutions a degree of discretion in how they comply with AML/ATF legislation and regulation, and on the procedures that they put in place for this purpose.
19. It is not intended that the guidance be applied unthinkingly, as a checklist of steps to take. Institutions should encourage their staff to 'think risk' as they carry out their duties within the legal and regulatory framework governing AML/ATF. The BMA expects institutions that it supervises to address their management of risk in a thoughtful and considered way, and establish and maintain systems and procedures that are appropriate and proportionate to the risks identified. This guidance assists institutions to do this.

The content of the guidance

20. This guidance emphasises the responsibility of senior management to manage the institution's money laundering and terrorist financing risks, and how this should be carried out on a risk-based approach. It sets out a standard approach to the identification and verification of customers, separating out basic identity from other aspects of customer due diligence measures, as well as giving guidance on the obligation to monitor customer activity.
21. This document also provides guidance to institutions on:
 - The importance of senior management taking responsibility for effectively managing the money laundering and terrorist financing risks faced by the institution's businesses (Chapter 1);
 - Appropriate controls in the context of financial crime (Chapter 2);
 - The role and responsibilities of the reporting officer (Chapter 3);
 - Adopting a risk-based approach to the application of customer due diligence measures (Chapter 4);
 - helping an institution have confidence that it has properly carried out its customer due diligence obligations, including monitoring customer transactions and activity (Chapter 5);
 - The identification and reporting of suspicious activity (Chapter 6);
 - Staff awareness, training and alertness (Chapter 7); and
 - Record keeping (Chapter 8)

Status of the guidance

22. The Court, or the Authority, as the case may be, in determining whether a person is in breach of a relevant provision of the Acts or Regulations, is required to consider whether a person has followed any relevant guidance issued by the Authority and approved by the Minister of Justice. This is detailed in the provisions of section 49A of POCA, regulation 19(2) of the Regulations 2008, section 12(B) of, and paragraph 1(6) of Part I of Schedule I to ATFA and section 20(6) of the SEA 2008. This guidance is also provided to assist institutions in complying with the various laws which assist in the prevention of Money Laundering and Terrorist Financing.
23. The guidance therefore provides a sound basis for institutions to meet their legislative and regulatory obligations when tailored by institutions to their particular business risk profile. Departures from this guidance, and the rationale for so doing, should be documented, and institutions will have to stand prepared to justify departures, for example to the BMA.

CHAPTER 1

GENERAL INSTITUTION AND SENIOR MANAGEMENT RESPONSIBILITIES

International recommendations and authorities

- FATF Forty Recommendations (June 2003, as amended October 2004).
- FATF Nine Special Recommendations on Terrorist Financing (revised October 2004).
- UN Security Council Resolutions 1267 (1999), 1373 (2001) and 1390 (2002).

International regulatory pronouncements

- Basel CDD paper.
- International Association of Insurance Supervisors (IAIS) Guidance Paper 5 on AML & CFT.
- International Organisation of Securities Commissions (IOSCO) Principles paper & Guidance on AML.
- Basel Consolidated KYC Risk Management.
- Wolfsberg Principles.
- FATF Guidance on the Risk Based Approach to Combating Money Laundering & Terrorist Financing.

Bermuda framework

Legislation

- Proceeds of Crime Act 1997.
- Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing) Regulations 2008.
- Financial Intelligence Agency Act 2007.
- Anti-Terrorism (Financial and Other Measures) Act 2004.
- Anti-Terrorism (Financial and Other Measures) (Business in Regulated Sector) Order 2008.
- Proceeds of Crime (Designated Countries and Territories) Order 1998.
- The Criminal Justice (International Cooperation) (Bermuda) Act 1994.
- The Terrorism (United Nations Measures) (Overseas Territories) Order 2001.
- The Al-Qa'ida and Taliban (United Nations Measures) (Overseas Territories) Order 2002.
- The Al-Qa'ida and Taliban (United Nations Measures) (Overseas Territories) (Amendment) Order 2002.
- Proceeds of Crime Regulations (Supervision and Enforcement) Act 2008.
- Guidance Notes for AML/ATF Regulated Financial Institutions on Anti-Money Laundering & Anti-Terrorist Financing.

Other Matters

- USA Patriot Act – extra territoriality.

Core obligations

Senior management in all institutions must:

- Ensure compliance with the Regulations;
- Identify, and manage effectively, the money laundering and terrorist financing risks in their businesses;
- Appoint a reporting officer to process disclosures;
- Ensure adequate resources are devoted to AML/ATF; and
- Recognise potential personal liability if legal obligations not met.

Introduction

- 1.1 Being used for money laundering or terrorist financing involves institutions in reputational, legal and regulatory risks. Senior management has a responsibility to ensure that the institution's control processes and procedures are appropriately designed and implemented, and are effectively operated to reduce the risk of the institution being used in connection with money laundering or terrorist financing.
- 1.2 Senior management in institutions are accustomed to applying proportionate, risk-based policies across different aspects of its business. An institution should therefore be able to take such an approach to the risk of being used for the purposes of money laundering or terrorist financing. Such an approach would change the emphasis and mindset towards money laundering and terrorist financing without reducing the effectiveness with which the risks are managed.
- 1.3 Under a risk-based approach, institutions start from the premise that most customers are not money launderers or terrorist financiers. However, institutions should have systems in place to highlight those customers who, on criteria established by the institution, may indicate that they present a higher-risk of this. The systems and procedures should be proportionate to the risks involved, and should be cost effective.
- 1.4 Senior management must be fully engaged in the decision-making processes, and must take ownership of the risk-based approach, since they may be held accountable if the approach is inadequate. That said, provided the assessment of the risks and the selection of mitigation procedures have been approached in a considered way, all the relevant decisions are properly recorded, and the institution's procedures are followed, the risk of censure should be very small.

International pressure to have effective AML/ATF procedures

- 1.5 Governments in many countries have enacted legislation to make money laundering and terrorist financing criminal offences, and have legal and regulatory processes in place to enable those engaged in these activities to be identified and prosecuted.
- 1.6 The Financial Action Task Force (FATF) have issued Forty Recommendations on Money Laundering aimed at setting minimum standards for action in different countries, to ensure that AML efforts are consistent internationally. FATF have also issued Nine Special Recommendations on Terrorist Financing, with the same broad objective as regards combating terrorist financing (CTF). The text of these Recommendations is available at www.fatf-gafi.org.
- 1.7 Internationally, the FATF Forty Recommendations, the Basel CDD paper, IAIS Guidance Paper 5 and the IOSCO Principles paper encourage national supervisors of financial entities to require institutions in their jurisdictions to follow specific due diligence procedures in relation to customers. In addition, the Basel Committee has issued a paper on Consolidated KYC Risk Management. These organisations explicitly envisage a risk-based approach to AML/ATF being followed by institutions.
- 1.8 The United Nations have sanctions in place to deny a range of named individuals and organisations, as well as nationals from certain countries, who it has been determined have been involved in money laundering and/or terrorist financing, access to the financial services sector.
- 1.9 The private sector Wolfsberg Group of banks has also published guidance in relation to Private Banking; Correspondent Banking; Suppression of the Financing of Terrorism; and Monitoring, Screening and Searching (collectively referred to as the Wolfsberg Principles).

Key elements of Bermuda's legal and regulatory AML/ATF framework are:

- Proceeds of Crime Act 1997;
- Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing) Regulations 2008;
- Anti-Terrorism (Financial and Other Measures) Act 2004;

- Anti-Terrorism (Financial and Other Measures) (Business in Regulated Sector) Order 2008;
- Proceeds of Crime (Designated Countries and Territories) Order 1998;
- The Criminal Justice (International Cooperation) (Bermuda) Act 1994;
- The Terrorism (United Nations Measures) (Overseas Territories) Order 2001;
- The Al-Qa'ida and Taliban (United Nations Measures) (Overseas Territories) Order 2002;
- The Al-Qa'ida and Taliban (United Nations Measures) (Overseas Territories) (Amendment) Order 2002;
- Bermuda Monetary Authority Act 1969;
- Proceeds of Crime Regulations (Supervision and Enforcement) Act 2008; and
- Guidance Notes on the Prevention of Money Laundering & Combating Terrorist Financing

1.10 Regulation of and guidance to institutions is provided by the BMA.

1.11 No single Bermuda body has overall responsibility for combating money laundering or terrorist financing. (Responsibilities are set out at Appendix II)

1.12 The Regulations apply to a range of specified institutions carrying on business in Bermuda. POCA and the ATFA have criminalised money laundering and terrorist financing respectively. Therefore, in considering their legal obligations, institutions need to think in terms of minimising the chance of inadvertent involvement with the proceeds of any crime or terrorist activity.

1.13 The BMA's objectives are to use regulatory measures to:

- Monitor AML/ATF regulated financial institutions to ensure full compliance with Bermuda's AML/ATF framework;
- Assist with the detection and prevention of financial crime; and
- Deter and disrupt criminal and terrorist activity by increasing the risk and lowering the reward faced by perpetrators.

1.14 In order to deliver these objectives successfully, the BMA believes action in this area must be underpinned by the three key organising principles:

Effectiveness – making maximum impact on the criminal and terrorist threat:

- Build knowledge of commercially effective compliance strategies to drive continuous improvement; and
- Make the best use of the regulatory tools we have, by making sure that all institutions make the maximum use of the opportunities provided by legislation, to prevent and detect AML/ATF threats.

Proportionality – so that the benefits of intervention are justified and that they outweigh the costs:

- Entrench the risk-based approach.

Engagement – so that all stakeholders in government and the private sector, at home and abroad, work collaboratively in partnership:

- Across the AML/ATF community, including to share data to reduce harm; and
- Engage international partners to deliver a global solution to a global problem.

General legal and regulatory obligations

Regulation 16

- 1.15 Senior management of any institution is responsible for managing its business effectively. Certain obligations are placed on all institutions subject to the Regulations - fulfilling these responsibilities falls to senior management as a whole.

Regulations 16 and 19(1)

- 1.16 The Regulations place a general obligation on institutions within its scope to establish adequate and appropriate policies and procedures to prevent money laundering and terrorist financing. An institution that fails to comply with this obligation risks regulatory enforcement action.

Regulation 19(1) & POCA S56 and ATFA S 5B

- 1.17 Where a body corporate is guilty of an offence under the POCA and/or ATFA and that offence is proved to have been committed with the consent or connivance of any director, manager, secretary or other similar officer of the body corporate or any person who was purporting to act in any such capacity, he, as well as the body corporate, shall be guilty of that offence and shall be liable to be proceeded against and punished accordingly.

Regulation 17 & 18 and POCA S46 and ATFA Schedule 1 Part 1

- 1.18 The offences of money laundering under POCA, and the obligation to report knowledge or suspicion of possible money laundering, affect all persons. Similar offences and obligations under the ATFA also affect all persons. In addition, institutions have an obligation under the Regulations to take appropriate measures so that all relevant employees are made aware of the law relating to money laundering and terrorist financing, and are regularly given training in how to recognise and deal with transactions which may be related to money laundering or terrorist financing.

Senior management should adopt a formal policy in relation to the prevention and detection of money laundering and terrorist financing

- 1.19 The BMA refers, in the context of setting its financial crime objectives, to the desirability of senior management of institutions being aware of the risk of their businesses being used in connection with the commission of financial crime, and taking appropriate measures to prevent financial crime and facilitate its detection. Senior management has operational responsibility for ensuring that the institution has appropriate systems and controls in place to combat financial crime.

- 1.20 In institutions supervised by the BMA a director or senior manager should be allocated overall responsibility for the establishment and maintenance of the institution's AML/ATF systems and controls.

- 1.21 Senior management of institutions supervised by the BMA should:

- Allocate to a director or senior manager overall responsibility for the establishment and maintenance of the institution's AML/ATF systems and controls;
- Appoint an appropriately qualified senior member of the institution's staff as the reporting officer (see Chapter 3); and
- Provide direction to, and oversight of, the institution's AML/ATF strategy.

- 1.22 Although it would be prudent that overall responsibility for AML/ATF systems and controls to be allocated to a single individual, in practice this may often be difficult to achieve, especially in larger institutions. As a practical matter, therefore, institutions may allocate this responsibility among a number of individuals, provided the division of responsibilities is clear.

- 1.23 The relationship between the reporting officer and the director/senior manager allocated overall responsibility for the establishment and maintenance of the institution's AML/ATF systems (where they are not the same person) is one of the keys to a successful AML/ATF regime. It is important that this relationship is clearly defined and documented, so that each knows the extent of his, and the other's, role and day-to-day responsibilities.
- 1.24 It would be prudent for an institution at least once in each calendar year, to commission a report from its compliance person on the operation and effectiveness of the institution's systems and controls to combat money laundering and terrorist financing. In practice, senior management should determine the depth and frequency of information they feel is necessary to discharge their responsibilities. The compliance person may also report to senior management more frequently than annually, as circumstances dictate.
- 1.25 When senior management receives such reports it should consider them and take any necessary action to remedy any deficiencies identified in a timely manner.
- 1.26 All institutions should apply adequate resources to counter the risk that they may be used for the purposes of financial crime. This includes systems and controls to prevent money laundering and terrorist financing. The level of resource should reflect the size, complexity and geographical spread of the institution's customer and product base.
- 1.27 The role, standing and competence of the compliance person and the reporting officer, and the way the internal systems, controls and processes and internal reporting procedures are designed and implemented, impact directly on the effectiveness of an institution's money laundering/terrorist financing prevention arrangements.
- 1.28 Institutions are encouraged to notify the BMA of the name and contact information of the reporting officer and compliance person and of any subsequent changes in the persons performing these functions. Receipt of such information will enhance the BMA's ability to communicate effectively with institutions on matters of mutual interest and provide a mechanism to communicate regulatory updates or advisories. Information can be forwarded using the email address: aml@bma.bm
- 1.29 As mentioned in paragraph 1.1 above, senior management in an institution supervised by the BMA for the purposes of AML/ATF compliance has a responsibility to ensure that the institution's control processes and procedures are appropriately designed and implemented, and are effectively operated to manage the institution's risks.
- 1.30 An institution should produce appropriate documentation of (its) risk management policies and risk profile in relation to money laundering and terrorist financing, including documentation of that institution's application of those policies. A statement of the institution's AML/ATF policy and the procedures to implement it will clarify how the institution's senior management intends to discharge its responsibility for the prevention of money laundering and terrorist financing. This will provide a framework of direction to the institution and its staff, and will identify named individuals and functions responsible for implementing particular aspects of the policy. The policy will also set out how senior management undertakes its assessment of the money laundering and terrorist financing risks the institution faces, and how these risks are to be managed. Even in a small institution, a summary of its high level AML/ATF policy will focus the minds of staff on the need to be constantly aware of such risks, and how they are to be managed.
- 1.31 A policy statement should be tailored to the circumstances of the institution and use of a generic document might reflect adversely on the level of consideration given by senior management to the institution's particular risk profile.
- 1.32 The policy statement might include, but not be limited to, such matters as:

Guiding principles:

- An unequivocal statement of the culture and values to be adopted and promulgated throughout the institution towards the prevention of financial crime;
- A commitment to ensuring that customers' identities will be satisfactorily verified before the institution accepts them;
- A commitment to the institution 'knowing its customers' appropriately - both at acceptance and throughout the business relationship - through taking appropriate steps to verify the customer's identity and business, and his reasons for seeking the particular business relationship with the institution;
- A commitment to ensuring that staff are trained and made aware of the law and their obligations under it, and to establishing procedures to implement these requirements; and
- Recognition of the importance of staff promptly reporting their suspicions internally.

Risk mitigation approach:

- A summary of the institution's approach to assessing and managing its money laundering and terrorist financing risk;
- Allocation of responsibilities to specific persons and functions;
- A summary of the institution's procedures for carrying out appropriate identification and monitoring checks on the basis of their risk-based approach; and
- A summary of the appropriate monitoring arrangements in place to ensure that the institution's policies and procedures are being carried out.

Application of group policies outside Bermuda

Regulation 12

- 1.33 The Bermuda legal and regulatory regime is primarily concerned with preventing money laundering and terrorist financing which is connected to Bermuda. Where a Bermuda institution has branches or subsidiary undertakings located in a country or territory other than Bermuda, it must require those branches or subsidiaries to apply, to the extent permitted by the law of that country or territory, measures at least equivalent to those set out in the Regulations with regard to customer due diligence, on-going monitoring and record keeping.

Regulation 12

- 1.34 A group policy must ensure that all branches and subsidiaries, located outside Bermuda, carry out customer due diligence measures, and keep records, at least to the standards required under Bermuda law or, if the standards in the host country are more rigorous, to those higher standards. Reporting processes must nevertheless follow local laws and procedures.
- 1.35 Where the law of a country or territory outside Bermuda does not permit the application of such equivalent measures, the institution must inform the BMA accordingly, and take additional measures to handle effectively the risk of money laundering or terrorist financing.

Regulation 16

- 1.36 Institutions must communicate their policies and procedures established to prevent activities related to money laundering and terrorist financing to branches and subsidiaries located outside Bermuda.

Criminal and Civil Penalties

- 1.37 Institutions should be aware that Regulation 19 of the Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing) Regulations 2008 provides that failure to comply with the requirements of a number of specified regulations is a criminal offence and carries with it significant penalties. On summary

conviction, a fine of up to \$50,000 and conviction on indictment, a fine of up to \$750,000 or imprisonment for a term of two years.

- 1.38 Further, Section 20 of the Proceeds of Crime Regulations (Supervision and Enforcement) Act 2008 empowers the BMA to impose a penalty on an AML/ATF regulated financial institution of up to \$500,000 for a failure to comply with the specified above regulations. The full details of the civil penalties process are contained in Chapter 4 of the Act. The Bermuda Monetary Authority has published a Statement of Principles which addresses the manner in which it proposes to exercise this power. The Act also provides for a number of criminal offences. In particular section 33 creates a three offences which carry significant penalties if convicted, either summarily or on indictment. The offences include carrying on business without being registered pursuant to section 9 of the Act.
- 1.39 In deciding whether a person has committed an offence against the regulations the court must consider whether any relevant guidance, issued at the time, was followed. The BMA must also consider whether any relevant guidance was followed when deciding if an institution has failed to comply with the regulations.
- 1.40 Where a person has been convicted of an offence under the regulations he shall not be liable to a civil penalty imposed by any other statutory provision in relation to the same matter.

USA Patriot Act – Extra-Territoriality

- 1.41 Where an institution has a US listing, or has activities in, or linked to, the USA, whether through a branch, subsidiary, associated company or correspondent banking relationship, there is a risk that the application of US AML/ATF and financial sanctions regimes may apply to the non-US activities of the institution. Senior management should take advice on the extent to which the institution's activities may be affected in this way.

CHAPTER 2

INTERNAL CONTROLS

Relevant law/regulation

Regulations 16 & 18

Core obligations

- AML/ATF regulated financial institutions must establish and maintain adequate and appropriate policies and procedures to forestall and prevent operations relating to money laundering and terrorist financing.
- Appropriate controls should take account of the risks faced by the institution's business.

Actions required, to be kept under regular review

- Establish and maintain adequate and appropriate policies and procedures to forestall and prevent money laundering and terrorist financing.
- Introduce appropriate controls to take account of the risks faced by the institution's business.
- Maintain appropriate control and oversight over outsourced activities.

General legal and regulatory obligations

Regulation 16

- 2.1 There is a requirement for institutions to establish and maintain appropriate and risk-based policies and procedures in order to prevent operations related to money laundering or terrorist financing.
- 2.2 This chapter provides guidance on the internal controls that will help institutions meet their obligations in respect of the prevention of money laundering and terrorist financing. There are prudential obligations on institutions to maintain appropriate records and controls more widely in relation to their business; this guidance is not intended to replace or interpret these wider obligations.

Appropriate controls in the context of financial crime prevention

Regulations 16 & 18

- 2.3 There are specific requirements under the Regulations for the institution to establish adequate and appropriate policies and procedures relating to: internal control; risk assessment and management (see Chapter 4); customer due diligence and on-going monitoring (see Chapter 5); record keeping (see Chapter 8); reporting of suspicious activity (see Chapter 6); the monitoring and management of compliance with such policies and procedures (see paragraph 3.11); and the internal communication of such policies and procedures (which includes staff awareness and training) (see Chapter 7). The Regulations are not specific about what these controls should comprise of but they must include measures for countering the risk that institutions will be used to facilitate money laundering or terrorist financing. The nature and extent of systems and controls will depend on a variety of factors, including:
 - The nature, scale and complexity of the institution's business;
 - The diversity of its operations, including geographical diversity;
 - Its customer, product and activity profile;
 - Its distribution channels;
 - The volume and size of its transactions; and
 - The degree of risk associated with each area of its operation.

- 2.4 Institutions must ensure that these systems and controls:
- Enable it to identify, assess, monitor and manage money laundering and terrorist financing risk; and
 - Are comprehensive and proportionate to the nature, scale and complexity of its activities.
- 2.5 An institution's systems and controls should cover senior management accountability, including allocation to a director or senior manager of overall responsibility for the establishment and maintenance of effective AML/ATF systems and controls and the appointment of persons with adequate seniority and experience as the compliance person and the reporting officer. The systems and controls should also cover:
- Appropriate training on money laundering and terrorist financing to ensure that employees are aware of, and understand, their legal and regulatory responsibilities and their role in money laundering/terrorist financing risk management;
 - Appropriate provision of regular and timely information to senior management relevant to the management of the institution's money laundering and terrorist financing risks;
 - Appropriate documentation of the institution's risk management policies and risk profile in relation to money laundering and terrorist financing, including documentation of the institution's application of those policies; and
 - Appropriate measures to ensure that money laundering and terrorist financing risk is taken into account in the day-to-day operation of the institution, including in relation to:
 - The development of new products;
 - The taking-on of new customers; and
 - Changes in the institution's business profile.

Outsourcing and non-Bermuda processing

- 2.6 A number of institutions outsource some of their systems and controls and/or processing to other jurisdictions, and/or to other group companies. Involving other entities in the operation of an institution's systems brings an additional dimension to the risks that the institution faces, and this risk must be actively managed. It is in the interests of the institution to ensure that outsourcing does not result in reduced standards or requirements being applied.
- 2.7 Institutions cannot contract out of their legal responsibilities, and therefore remain responsible for systems and controls in relation to the activities outsourced. In all instances of outsourcing it is the delegating institution that bears the ultimate responsibility for the duties undertaken in its name. This will include the requirement to ensure that the provider of the outsourced services has in place satisfactory AML/ATF systems, controls and procedures, and that those policies and procedures are kept up-to-date to reflect changes in Bermuda requirements.
- 2.8 Where Bermuda operational activities are undertaken by staff in other jurisdictions (for example, overseas call centres), those staff should be subject to the AML/ATF policies and procedures that are applicable to Bermuda staff and internal reporting procedures implemented to ensure that all suspicions relating to Bermuda-related accounts, transactions or activities are reported to the reporting officer in Bermuda.
- 2.9 Institutions should also be aware of local obligations, in all jurisdictions to which they outsource functions, for the detection and prevention of financial crime. Procedures should be in place to meet local AML/ATF regulations and reporting requirements. Any conflicts between Bermuda and local AML/ATF requirements, where meeting local requirements would result in a lower standard than in Bermuda, should be resolved in favour of Bermuda.
- 2.10 In some circumstances, the outsourcing of functions can actually lead to increased risk - for example, outsourcing to businesses in jurisdictions with less stringent AML/ATF requirements than in Bermuda. All institutions that outsource functions and activities should therefore assess any possible money laundering or

terrorist financing risk associated with the outsourced functions, record the assessment, monitor the risk and implement policies and procedures to minimise that risk as appropriate on an on-going basis.

CHAPTER 3

REPORTING OFFICER

Relevant law/regulation

Regulation 16 & 17

Core obligations

- Reporting officer must receive and review internal disclosures, and make external reports.
- Reporting officer is responsible for making external reports.
- Reporting officer should be able to act on his own authority.
- Adequate resources must be devoted to AML/ATF.

Actions required, to be kept under regular review

Senior management to ensure the reporting officer:

- Has active support of senior management;
- Has adequate resources;
- Has independence of action; and
- Has access to information

General legal and regulatory obligations

Regulation 16 & 17

- 3.1 All institutions (other than sole traders) must appoint a reporting officer.
- 3.2 The reporting officer is responsible for receiving disclosures under section 46 of the Proceeds of Crime Act 1997 and Schedule 1 Part 1 of the Anti-Terrorism (Financial and Other Measures) Act 2004 and deciding whether these should be reported to the Financial Intelligence Agency, and, if appropriate, making such external reports.
- 3.3 The reporting officer should have the authority to act independently in carrying out his responsibilities. The reporting officer should be free to have direct access to the BMA and where appropriate law enforcement agencies, in order that any suspicious activity may be reported to the right quarter as soon as is practicable. He must be free to liaise with the Financial Intelligence Agency on any question of whether to proceed with a transaction in the circumstances.
- 3.4 Senior management of the institution must ensure that the reporting officer has sufficient resources available to him, including appropriate staff and technology. This should include arrangements to apply in his temporary absence.
- 3.5 Where an institution is part of a group, it may appoint as its reporting officer an individual who performs that function for another institution within the group. If an institution chooses this approach, it may wish to permit the reporting officer to delegate AML/ATF duties to other suitably qualified individuals within the institution. Similarly, some institutions, particularly those with a number of branches or offices in different locations, may wish to permit the reporting officer to delegate such duties within the institution. In larger institutions, because of their size and complexity, the appointment of one or more permanent deputy reporting officers of suitable seniority may be necessary. In such circumstances, the principal, or group reporting officer needs to ensure that roles and responsibilities within the group are clearly defined, so that staff of all business areas know exactly who they must report suspicions to.

Internal and external reports

Regulation 17

- 3.6 An institution must require that anyone in the institution to whom information or other matter comes in the course of business as a result of which they know or suspect, that a person is engaged in money laundering or terrorist financing, complies with section 46 of the Proceeds of Crime Act 1997 or Schedule 1 Part 1 of the Anti-Terrorism (Financial and Other Measures) Act 2004 (as the case may be). This includes staff having an obligation to make an internal report to the reporting officer as soon as is reasonably practicable after the information or other matter comes to them.
- 3.7 Any internal report should be considered by the reporting officer, in the light of all other relevant information, to determine whether or not the information contained in the report does give rise to knowledge or suspicion of money laundering or terrorist financing.
- 3.8 An institution is expected to use its existing customer information effectively by making such information readily available to its reporting officer.
- 3.9 In most cases, before deciding to make a report, the reporting officer is likely to need access to the institution's relevant business information. An institution should therefore take reasonable steps to give its reporting officer access to such information. Relevant business information may include details of:
- The financial circumstances of a customer or beneficial owner, or any person on whose behalf the customer has been or is acting; and
 - The features of the transactions, including, where appropriate, the jurisdiction in which the transaction took place, which the institution entered into with or for the customer (or that person).
- 3.10 In addition, the reporting officer may wish:
- To consider the level of identity information held on the customer, and any information on his personal circumstances that might be available to the institution; and
 - To review other transaction patterns and volumes through the account or accounts in the same name, the length of the business relationship and identification records held.
- 3.11 If the reporting officer concludes that the internal report does give rise to knowledge or suspicion of money laundering or terrorist financing, he must make a report to the Financial Intelligence Agency as soon as is reasonably practicable after he makes this determination.
- 3.12 Guidance on reviewing internal reports, and reporting as appropriate to the Financial Intelligence Agency, is set out in (Chapter 6).

National and international findings in respect of countries and jurisdictions

- 3.13 An institution should ensure that it obtains and makes appropriate use of, any government, FATF, CFATF or other like regional body's findings concerning the approach to the prevention of money laundering or terrorist financing in particular countries or jurisdictions. This is especially relevant where the approach has been found to be materially deficient following an internationally recognised assessment by the FATF or like body. Reports on the mutual evaluations carried out by the CFATF or FATF can be found at www.cfatf.org or www.fatf-gafi.org. FATF-style regional bodies also evaluate their members. Not all evaluation reports are published and where an evaluation has been carried out and the findings are not published, institutions will take this fact into account in assessing the money laundering and terrorist financing risks posed by the jurisdiction in question. Depending on the institution's area of operation, it may be appropriate to take account of other international findings, such as those by the IMF or World Bank.

- 3.14 Institutions considering business relations and transactions with individuals and institutions – whether direct or through correspondents - located in higher-risk jurisdictions, should take account of the background against which the assessment has been made.

Monitoring effectiveness of money laundering controls

Regulation 16(1)(f)

- 3.15 An institution is required to carry out regular assessments of the adequacy of its systems and controls to ensure that they manage the money laundering and terrorist financing risk effectively. Oversight of the implementation of the institution's AML/ATF policies and procedures, including the operation of the risk-based approach, should be the responsibility of the compliance person, but may be appropriately delegated. He should therefore ensure that appropriate monitoring processes and procedures across the institution are established and maintained.

Reporting to senior management

- 3.16 As noted in paragraph 1.24, the relationship between the reporting officer and the director(s)/senior manager(s) allocated overall responsibility for the establishment and maintenance of the institution's AML/ATF systems (where they are not the same person) is one of the keys to a successful AML/ATF regime. It is important that this relationship is clearly defined and documented, so that each knows the extent of his, and the other's, role and day-to-day responsibilities.
- 3.17 At least annually the senior management of a BMA supervised institution should commission a report which assesses the operation and effectiveness of the institution's systems and controls in relation to managing money laundering and terrorist financing risk.
- 3.18 In practice, senior management should determine the depth and frequency of information they feel necessary to discharge their responsibilities and ensure reports are provided as frequently as circumstances dictate.
- 3.19 The institution's senior management should consider the report, and take any necessary action to remedy deficiencies identified in it, in a timely manner.
- 3.20 Such reports should bring to the attention of senior management areas where the operation of AML/ATF controls should be improved, and proposals for making appropriate improvements. The progress of any significant remedial programmes will also be reported to senior management.
- 3.21 In addition, such reports should include the outcome of any relevant quality assurance or internal audit reviews of the institution's AML/ATF processes, as well as the outcome of any review of the institution's risk assessment procedures (see paragraph 4.34).
- 3.22 Institutions will need to use their judgement as to content and format of the annual compliance report which will include a section from the reporting officer and a breakdown of the statistics regarding internal and external reports.

CHAPTER 4

RISK-BASED APPROACH

Relevant law/regulation

Regulation 6(3)(a)

Other authoritative pronouncements which endorse a risk-based approach

- FATF Recommendation 5.
- Basel CDD Paper.
- IAIS Guidance Paper 5.
- IOSCO Principles paper.
- Basel Consolidated KYC Risk Management Paper.
- FATF - Guidance on the Risk Based approach to combating Money Laundering and Terrorist Financing.

Core obligations

- Appropriate systems and controls must reflect the degree of risk associated with the business and its customers.
- Determine appropriate customer due diligence (“CDD”) measures on a risk-sensitive basis, depending on the type of customer, business relationship, product or transaction. (see Chapter 5).
- Take into account situations which by their nature can present a higher-risk of money laundering or terrorist financing; these specifically include where the customer has not been physically present for identification purposes; correspondent banking relationships; and business relationships and occasional transactions with politically exposed persons (“PEPs”). (see paragraphs 5.231 – 5.244).

Actions required, to be kept under regular review

- Carry out a formal, and regular, money laundering/terrorist financing risk assessment, including market changes, and changes in products, customers and the wider environment.
- Ensure internal procedures, systems and controls, including staff awareness, adequately reflect the risk assessment.
- Ensure customer identification and acceptance procedures reflect the risk characteristics of customers.
- Ensure arrangements for monitoring systems and controls are robust, and reflect the risk characteristics of customers.

Introduction

4.1 Senior management of most institutions, whatever business they are in, manages its affairs with regard to the risks inherent in its business and the effectiveness of the controls it has put in place to manage these risks. A similar approach is appropriate to managing the risks of the institution being used for money laundering or terrorist financing. Many authoritative international bodies operating in the financial services sector have issued pronouncements endorsing, and encouraging institutions to follow, a risk-based approach to managing money laundering/terrorist financing risk.

4.2 A risk-based approach takes a number of discrete steps in assessing the most cost effective and proportionate way to manage and mitigate the money laundering and terrorist financing risks faced by the institution. These steps are to:

- Identify the money laundering and terrorist financing risks that are relevant to the institution;
- Assess the risks presented by the institution’s particular:
 - Customers;
 - Products;
 - Delivery channels;

- Geographical areas of operation;
 - Design and implement controls to manage and mitigate these assessed risks;
 - Monitor and improve the effective operation of these controls; and
 - Record appropriately what has been done, and why.
- 4.3 No system of checks will detect and prevent all money laundering or terrorist financing. A risk-based approach will, however, serve to balance the cost burden placed on individual institutions and their customers with a realistic assessment of the threat of the institution being used in connection with money laundering or terrorist financing. It focuses the effort where it is needed and will have most impact.
- 4.4 To assist the overall objective to prevent money laundering and terrorist financing, a risk-based approach:
- Recognises that the money laundering/terrorist financing threat to institutions varies across customers, jurisdictions, products and delivery channels;
 - Allows management to differentiate between their customers in a way that matches the risk in their particular business;
 - Allows senior management to apply its own approach to the institution's procedures, systems and controls, and arrangements in particular circumstances; and
 - Helps to produce a more cost effective system.
- 4.5 The appropriate approach in any given case is ultimately a question of judgement by senior management, in the context of the risks they consider the institution faces. If an institution demonstrates that it has put in place an effective system of controls that identifies and mitigates its money laundering and terrorist financing risk, then enforcement action by the BMA is unlikely. The BMA recognises that any regime that is risk-based cannot be a zero failure regime not least because a 100% standard will not be cost-effective and will damage innovation, competition and legitimate commercial success.

A risk-based approach

- 4.6 All institutions must assess their money laundering/terrorist financing risk in some way and decide how they will manage it. Institutions may choose to carry out this assessment in a sophisticated way, or in a more simple way, having regard to the business they undertake, their customer base and their geographical area of operation. There is no requirement, or expectation, that a risk-based approach must involve a complex set of procedures to put it into effect; the particular circumstances of the institution will determine the most appropriate approach.
- 4.7 The business of many institutions, their product and customer base, can be relatively simple, involving few products, with most customers falling into similar categories. In such circumstances, a simple approach, building on the risk the institution's products are assessed to present, may be appropriate for most customers, with the focus being on those customers who fall outside the 'norm'. Other institutions may have a greater level of business, but large numbers of their customers may be predominantly retail, served through delivery channels that offer the possibility of adopting a standardised approach to many AML/ATF procedures. Here, too, the approach for most customers may be relatively straightforward, building on the product risk.
- 4.8 Some other institutions, however, often (but not exclusively) those dealing in wholesale markets, may offer a more 'bespoke' service to customers, many of whom are already subject to extensive due diligence by lawyers and accountants for reasons other than AML/ATF. In such cases, the business of identifying the customer will be more complex, but will take account of the considerable additional information that already exists in relation to the prospective customer.
- 4.9 How a risk-based approach is implemented will also depend on the institution's operational structure. For example, an institution that operates through multiple business units will need a different approach from one that operates as a single business.
- 4.10 Whatever approach is considered most appropriate to the institution's money laundering/terrorist financing risk, the broad objective is that the institution should know who their customers are, what they do, and

whether or not they are likely to be engaged in criminal activity. The profile of their financial behaviour will build up over time, allowing the institution to identify transactions or activity that may be suspicious.

- 4.11 However carried out, a risk-based approach requires the full commitment and support of senior management, and the active co-operation of business units. The risk-based approach needs to be part of the institution's philosophy, and as such reflected in its procedures and controls. There needs to be clear communication of policies and procedures across the institution, along with robust mechanisms to ensure that they are carried out effectively, weaknesses are identified, and improvements are made wherever necessary.
- 4.12 A risk assessment will often result in a stylised categorisation of risk: e.g., high/medium/low. Criteria will be attached to each category to assist in allocating customers and products to risk categories, in order to determine the different treatments of identification, verification, additional customer information and monitoring for each category, in a way that minimises complexity.

Identifying and assessing the risks faced by the institution

- 4.13 Senior management should decide on the appropriate approach in the light of the institution's structure. The institution may adopt an approach that starts at the business area level, or one that starts from business streams. The institution may start with its customer assessments, and overlay these assessments with the product and delivery channel risks; or it may choose an approach that starts with the product risk, with the overlay being the customer and delivery channel risks, taking account of any geographical considerations relating to the customer, or the transaction.
- 4.14 A risk-based approach starts with the identification and assessment of the risk that has to be managed.

Regulation 16(2)(a)

What risk is posed by the institution's customers? For example:

- Complex business ownership structures, which can make it easier to conceal underlying beneficiaries, where there is no legitimate commercial rationale;
- An individual meeting the definition of a PEP;
- Customers (not necessarily PEPs) based in, or conducting business in or through, a high-risk jurisdiction, or a jurisdiction with known higher levels of corruption or organised crime, or drug production/distribution; and
- Customers engaged in a business which involves significant amounts of cash, or which are associated with higher levels of corruption (e.g. arms dealing).

What risk is posed by a customer's behaviour? For example:

- Where there is no commercial rationale for the customer buying the product he seeks;
- Requests for a complex or unusually large transaction which has no apparent economic or lawful purpose;
- Requests to associate undue levels of secrecy with a transaction;
- Situations where the origin of wealth and/or source of funds cannot be easily verified or where the audit trail has been deliberately broken and/or unnecessarily layered; and
- The unwillingness of customers who are not private individuals to give the names of their real owners and controllers.

How does the way the customer comes to the institution affect the risk? For example:

- Occasional transactions (see paragraph 5.29) versus business relationships (see paragraph 5.28);
- Introduced business, depending on the effectiveness of the due diligence carried out by the introducer; and
- Non face-to-face acceptance.

What risk is posed by the products/services the customer is using? For example:

- Can the product features be used for money laundering or terrorist financing, or to fund other crime?
- Do the products allow/facilitate payments to third parties?
- Is the main risk that of inappropriate assets being placed with, or moving from, or through, the institution?
- Does a customer migrating from one product to another within the institution carry a risk?

4.17 Many customers, by their nature or through what is already known about them by the institution, carry a lower money laundering or terrorist financing risk. These might include:

- Customers who are employment-based or with a regular source of income from a known source which supports the activity being undertaken; (this applies equally to pensioners or benefit recipients, or to those whose income originates from their partners' employment);
- Customers with a long-term and active business relationship with the institution; and
- Customers represented by those whose appointment is subject to court approval or ratification (such as executors).

4.18 Institutions should not, however, judge the level of risk solely on the nature of the customer or the product. Where, in a particular customer/product combination, *either or both* the customer and the product are considered to carry a higher-risk of money laundering or terrorist financing, the overall risk of the customer should be considered carefully. Institutions need to be aware that allowing a higher-risk customer to acquire a lower-risk product or service on the basis of a verification standard that is appropriate to that lower-risk product or service, can lead to a requirement for further verification requirements, particularly if the customer wishes subsequently to acquire a higher-risk product or service.

Design and implement controls to manage and mitigate the risks

4.19 Once the institution has identified and assessed the risks it faces in respect of money laundering or terrorist financing, senior management must ensure that appropriate controls to manage and mitigate these risks are designed and implemented.

Regulation 6(3)(a)

4.20 As regards money laundering and terrorist financing, managing and mitigating the risks will involve measures to verify the customer's identity, collecting additional information about the customer and monitoring his transactions and activity to determine whether there is a knowledge or suspicion that money laundering or terrorist financing may be taking place. Part of the control framework will involve decisions as to whether verification should take place electronically, and the extent to which the institution can use customer verification procedures carried out by other institutions. Institutions must determine the extent of their customer due diligence measures on a risk-sensitive basis depending on the type of customer, business relationship, product or transaction.

4.21 To decide on the most appropriate and relevant controls for the institution, senior management should ask themselves what measures the institution can adopt, and to what extent, to manage and mitigate these threats/risks most cost effectively, and in line with the institution's risk appetite. Examples of control procedures include:

- Introducing a customer identification programme that varies the procedures in respect of customers appropriate to their assessed money laundering/terrorist financing risk;
- Requiring the quality of evidence - documentary/electronic/third party assurance - to be of a certain standard;
- Obtaining additional customer information, where this is appropriate to their assessed money laundering/terrorist financing risk; and
- Monitoring customer transactions/activities.

- 4.22 It is possible to try to assess the extent to which each customer should be subject to each of these checks, but it is the balance of these procedures as appropriate to the risk assessed in the individual customer, or category of customer, to which he belongs that is relevant.
- 4.23 A customer identification programme that is graduated to reflect risk could involve:
- A standard information dataset to be held in respect of all customers;
 - A standard verification requirement for all customers;
 - More extensive due diligence (more identification checks and/or requiring additional information) on customer acceptance for higher-risk customers;
 - Where appropriate, more limited identity verification measures for specific lower-risk customer/product combinations; and
 - An approach to monitoring customer activities and transactions that reflects the risk assessed to be presented by the customer, which will identify those transactions or activities that may be unusual or suspicious.
- 4.24 Where a customer is assessed as carrying a higher risk, then depending on the product sought, it will be necessary to seek additional information in respect of the customer, to be better able to judge whether or not the higher-risk that the customer is perceived to present is likely to materialise. Such additional information may include an understanding of where the customer's funds and wealth have come from. (Guidance on the types of additional information that may be sought is set out in paragraphs 5.216 to 5.244).
- 4.25 In order to be able to identify customer transactions or activity that may be suspicious, it is necessary to monitor such transactions or activity in some way. Guidance on monitoring customer transactions and activity is given in paragraphs 5.283 to 5.303. Monitoring customer activity should be carried out on the basis of a risk-based approach, with higher-risk customer/product combinations being subjected to an appropriate frequency and depth of scrutiny, which is likely to be greater than may be appropriate for lower-risk combinations.
- 4.26 The institution must decide, on the basis of its assessment of the risks posed by different customer/product combinations, on the level of verification that should be applied at each level of risk presented by the customer. Consideration should be given to all the information an institution gathers about a customer, as part of the normal business and vetting processes. Consideration of the overall information held may alter the risk profile of the customer.
- 4.27 Identifying a customer as carrying a higher risk of money laundering or terrorist financing does not automatically mean that he is a money launderer, or a financier of terrorism. Similarly, identifying a customer as carrying a low risk of money laundering or terrorist financing does not mean that the customer is not. Staff, therefore need to be vigilant in using their experience and common sense in applying the institution's risk-based criteria and rules (see Chapter 7 – Staff awareness, training and alertness).

Monitor and improve the effective operation of the institution's controls

- 4.28 The institution will need to have some means of assessing that its risk mitigation procedures and controls are working effectively, or, if they are not, where they need to be improved. Its policies and procedures will need to be kept under regular review. Aspects the institution will need to consider include:
- Appropriate procedures to identify changes in customer characteristics, which come to light in the normal course of business;
 - Reviewing ways in which different products and services may be used for money laundering/terrorist financing purposes, and how these ways may change, supported by typologies/law enforcement feedback, etc;
 - Adequacy of staff training and awareness;
 - Monitoring compliance arrangements (such as internal audit/quality assurance processes or external review);

- The balance between technology-based and people-based systems;
- Capturing appropriate management information;
- Upward reporting and accountability;
- Effectiveness of liaison with other parts of the institution; and
- Effectiveness of the liaison with regulatory and law enforcement agencies.

Record appropriately what has been done and why

- 4.29 The responses to consideration of the issues set out above, or to similar issues, will enable the institution to tailor its policies and procedures on the prevention of money laundering and terrorist financing. Documentation of those responses should enable the institution to demonstrate to the BMA:
- How it assesses the threats/risks of being used in connection with money laundering or terrorist financing;
 - How it agrees and implements the appropriate systems and procedures, including due diligence requirements, in the light of its risk assessment;
 - How it monitors and, as necessary, improves the effectiveness of its systems and procedures; and
 - The arrangements for reporting to senior management on the operation of its control processes.

Risk management is dynamic

- 4.30 Risk management generally is a continuous process, carried out on a dynamic basis. A money laundering/terrorist financing risk assessment is not a one-time exercise. Institutions must therefore ensure that their risk management processes for managing money laundering and terrorist financing risks are kept under regular review.
- 4.31 There is a need to monitor the environment within which the institution operates. Success in preventing money laundering and terrorist financing in one area of operation or business will tend to drive criminals to migrate to another area, business, or product stream. Periodic assessment should therefore be made of activity in the institution's market place. If displacement is happening, or if customer behaviour is changing, the institution should be considering what it should be doing differently to take account of these changes.
- 4.32 In a stable business change may occur slowly: most businesses are evolutionary. Customers' activities change (without always notifying the institution) and the institution's products and services – and the way these are offered or sold to customers – change. The products/transactions attacked by prospective money launderers or terrorist financiers will also vary as perceptions of their relative vulnerability change.
- 4.33 There is, however, a balance to be achieved between responding promptly to environmental changes, and maintaining stable systems and procedures.
- 4.34 An institution should therefore keep its risk assessment(s) up to date. An annual, formal reassessment might be too often in most cases, but still appropriate for a dynamic, growing business. It is recommended that an institution revisit its assessment at least annually, even if it decides that there is no case for revision. Institutions should include details of the assessment, and any resulting changes when reporting to senior management.

CHAPTER 5

CUSTOMER DUE DILIGENCE

Relevant Bermuda law/regulation

- Proceeds of Crime Act 1997.
- Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing) Regulations 2008.
- Anti-Terrorism (Financial and Other Measures) Act 2004.
- Anti-Terrorism (Financial and Other Measures) (Business in Regulated Sector) Order 2008.

Customers that may not be dealt with

- UN Sanctions resolutions 1267 (1999), 1373 (2001), 1390 (2002) and 1617 (2005).
- The Terrorism (United Nations Measures) (Overseas Territories) Order 2001.
- The Al-Qa'ida and Taliban (United Nations Measures) (Overseas Territories) Order 2002.
- The Al-Qa'ida and Taliban (United Nations Measures) (Overseas Territories) (Amendment) Order 2002.

Other material pointing to good practice

- FATF Recommendations.
- FATF Guidance on the risk-based approach: High level principles and procedures.
- Basel customer due diligence paper.
- IAIS Guidance Paper 5.
- IOSCO Principles paper.
- Basel Consolidated KYC Risk Management Paper.

Other relevant industry material

- Wolfsberg Principles.

Core obligations

- Must carry out prescribed customer due diligence measures for all customers not covered by exemptions.
- Must have systems to deal with identification issues in relation to those who cannot produce the standard evidence.
- Must apply enhanced due diligence to take account of the greater potential for money laundering or terrorist financing in higher-risk cases, specifically when the customer is not physically present when being identified, in respect of PEPs and correspondent banking relationships.
- If satisfactory evidence of identity is not obtained, the business relationship must not proceed further.
- Must have some system for keeping customer information, so far as practicable, up-to-date.

Meaning of customer due diligence measures and on-going monitoring

- 5.1 The Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing) Regulations 2008, which came into force on the 1st January 2009, replace the previous Proceeds of Crime (Money Laundering) Regulations 1998. The 2008 Regulations set out an institutions' obligations to conduct customer due diligence measures in a more detailed form than previously.
- 5.2 The Regulations specify customer due diligence measures that are required to be carried out, and the timing, as well as actions required if customer due diligence measures are not carried out. The Regulations then describe customers and products in respect of which no, or limited, customer due diligence measures are required (referred to as 'Simplified Due Diligence'), and those customers and circumstances where enhanced due diligence is required. Provision for reliance on third parties in the carrying out of customer due diligence measures are also set out.

5.3 This chapter therefore gives guidance on the following:

- The meaning of customer due diligence measures - Regulation 5;
- Timing of, and non-compliance with, customer due diligence measures – Regulation 8;
- Application of customer due diligence measures – Regulation 6;
- Simplified due diligence – Regulation 10;
- Enhanced due diligence – Regulation 11;
- Reliance on third parties and multipartite relationships – Regulation 14; and
- Monitoring customer activity – Regulation 7.

Regulation 6(3) (a) & 7(3)

5.4 Institutions must determine the extent of their customer due diligence measures and on-going monitoring on a risk-sensitive basis, depending on the type of customer, business relationship, product or transaction. They must be able to demonstrate to the BMA that the extent of their customer due diligence measures and monitoring is appropriate in view of the risks of money laundering and terrorist financing.

What is customer due diligence?

Regulation 5

5.5 The customer due diligence measures that must be carried out involve:

- Identifying the customer, and verifying his identity (see paragraphs 5.25 to 5.30);
- Identifying the beneficial owner, where relevant, and verifying his identity (see paragraphs 5.31 to 5.36); and
- Obtaining information on the purpose and intended nature of the business relationship (see paragraphs 5.43 & 5.44).

Regulation 5(b)

5.6 Where the customer is a legal person (such as a company) or a legal arrangement (such as a trust), part of the obligation on an institution to identify any beneficial owner of the customer is taking measures to understand the ownership and control structure of the customer.

5.7 Working out who is a beneficial owner may not be a straightforward matter. Different rules apply to different forms of entity (see paragraph 5.31).

Regulations 10 & 11

5.8 For some particular customers, products or transactions, simplified due diligence (“SDD”) may be applied. In the case of higher-risk situations, and specifically in relation to customers who are not physically present when their identities are verified, correspondent banking and PEPs, enhanced due diligence (“EDD”) measures must be applied on a risk sensitive basis.

- For guidance on applying simplified due diligence (see paragraphs 5.209 to 5.215).
- For guidance on applying enhanced due diligence (see paragraphs 5.216 to 5.223).

What is on-going monitoring?

Regulation 7

5.9 Institutions must conduct on-going monitoring of the business relationship with their customers. This is a separate, but related, obligation from the requirement to apply customer due diligence measures. Ongoing monitoring of a business relationship means the scrutiny of transactions undertaken throughout the course of the relationship (including, where necessary, the source of funds) to ensure that the transactions are

consistent with the relevant person's knowledge of the customer, his business and risk profile and so far as practicable keeping the documents, data or information obtained for the purpose of applying customer due diligence measures up-to-date.

Why is it necessary to apply customer due diligence measures and conduct on-going monitoring?

Regulations 6 & 7

- 5.10 The customer due diligence and monitoring obligations on institutions under the regulations are designed to make it more difficult for the institutions to be used for money laundering or terrorist financing.
- 5.11 Institutions also need to know who their customers are, to guard against fraud including impersonation fraud and the risk of committing offences under POCA and the ATFA, relating to money laundering and terrorist financing.
- 5.12 Institutions therefore need to carry out customer due diligence and monitoring for two broad reasons:
- To help the institution at the time due diligence is carried out, to be reasonably satisfied that customers are who they say they are, to know whether they are acting on behalf of another, and that there is no legal barrier (e.g. sanctions) to providing them with the product or service requested; and
 - To enable the institution to assist law enforcement by providing available information on customers or activities being investigated.
- 5.13 It may often be appropriate for the institution to know rather more about the customer than his identity: it will, for example, often need to be aware of the nature of the customer's business in order to assess the extent to which his transactions and activity undertaken with or through the institution is consistent with that business.

Other material, pointing to good practice

- 5.14 FATF, the Basel Committee, IAIS and IOSCO have issued recommendations on the steps that should be taken to identify customers. FATF has also published guidance on high level principles and procedures on the risk-based approach. In addition, the Basel Committee has issued a paper on Consolidated KYC Risk Management. Although the Basel papers are addressed to banks, the IAIS Guidance Paper 5 to insurance entities, and IOSCO's Principles paper to the securities industry, their principles are worth considering by providers of other forms of financial services. The private sector Wolfsberg Group has also issued relevant material. These recommendations are available at: www.fatf-gafi.org; www.bis.org; www.iaisweb.org; www.iosco.org; www.wolfsberg-principles.com. Where relevant, institutions are encouraged to use these websites to keep up-to-date with developing industry guidance from these bodies.

Timing of, and non compliance with, customer due diligence measures

Regulation 7

- 5.15 An institution must apply customer due diligence measures when it:
- Establishes a business relationship;
 - Carries out an occasional transaction;
 - Suspects money laundering or terrorist financing; or
 - Doubts the veracity of documents, data or information previously obtained for the purpose of identification or verification.

Timing of verification

Regulation 8(2)

- 5.16 **General rule** - the verification of the identity of the customer and where applicable, the beneficial owner, must, subject to the exceptions referred to below, take place before the establishment of a business relationship or the carrying out of an occasional transaction.

Regulation 8(4)

- 5.17 **Exception for life assurance** - the verification of the identity of the beneficiary under a life assurance policy may take place after the business relationship has been established provided that it takes place at or before the time of payout or at or before the time the beneficiary exercises a right vested under the policy.

Regulation 8(5)

- 5.18 **Exception when opening a bank account** - the verification of the identity of a bank account holder may take place after the bank account has been opened, provided that there are adequate safeguards in place to ensure that:

- The account is not closed; and
- Transactions are not carried out by or on behalf of the account holder (including any payment from the account to the account holder) before verification has been completed.

Regulation 8(3)

- 5.19 **Exception if necessary not to interrupt normal business and there is little risk** - in any other case, verification of the identity of the customer, and where there is one, the beneficial owner, may be completed during the establishment of a business relationship if:

- This is necessary not to interrupt the normal conduct of business; and
- There is little risk of money laundering or terrorist financing occurring provided that the verification is completed as soon as practicable after the initial contact.

Requirement to cease transactions, etc.

Regulation 9(1)

- 5.20 Where an institution is unable to apply customer due diligence measures in relation to a customer, the institution:

- Shall not carry out a transaction with or for the customer through a bank account;
- Shall not establish a business relationship or carry out an occasional transaction with the customer;
- Shall terminate any existing business relationship with the customer; and
- Shall consider whether it ought to be making a report to the Financial Intelligence Agency, in accordance with its obligations under POCA and the ATFA.

- 5.21 Institutions should always consider whether an inability to apply customer due diligence measures is caused by the customer not possessing the 'right' documents or information. In this case the institution should consider whether there are any other ways of being reasonably satisfied as to the customer's identity. In either case the institution should consider whether there are any circumstances which give grounds for making a report.

- 5.22 If the institution concludes that the circumstances do give rise to a knowledge or suspicion of money laundering or terrorist financing, a report must be made to the Financial Intelligence Agency (see Chapter 6). The institution must then retain the funds until consent has been given to return the funds to the source from which they came.

- 5.23 If the institution concludes that there are no grounds for making a report, it will need to decide on the appropriate course of action. This may be to retain the funds while it seeks other ways of being reasonably satisfied as to the customer's identity, or to return the funds to the source from which they came. Returning the funds in such a circumstance is part of the process of terminating the relationship; it is closing the account, rather than carrying out a transaction with the customer through a bank account.

Application of customer due diligence measures

Regulation 5

- 5.24 Applying customer due diligence measures involves several steps. The institution is required to identify customers and, where applicable, beneficial owners. It must then verify these identities. Information on the purpose and intended nature of the business relationship must also be obtained.

Identification and verification of the customer

- 5.25 The institution *identifies* the customer by obtaining a range of information about him. The *verification* of the identity consists of the institution verifying some of this information against documents, data or information obtained from a reliable and independent source.
- 5.26 The term 'customer' is not defined in the Regulations and its meaning has to be inferred from the definitions of 'business relationship' and 'occasional transaction', the context in which it is used in the Regulations, and its everyday dictionary meaning.
- 5.27 In general the customer will be the party, or parties, with whom the business relationship is established, or for whom the transaction is carried out. Where, however, there are several parties to a transaction, not all will necessarily be customers.

Regulation 2(1)

- 5.28 A "**business relationship**" is defined in the Regulations as a business, professional or commercial relationship between an institution and a customer, which is expected by the institution when contact is first made between them to have an element of duration. A relationship need not involve the institution in an actual transaction; giving advice may often constitute establishing a business relationship.

Regulation 2(1)

- 5.29 An "**occasional transaction**" means a transaction carried out other than in the course of a business relationship (e.g. a single foreign currency transaction, or an isolated instruction to purchase shares), amounting to \$15,000 or more, whether the transaction is carried out in a single operation or several operations which appear to be linked.
- 5.30 The factors linking transactions to assess whether there is a business relationship are inherent in the characteristics of the transactions – for example, where several payments are made to the same recipient from one or more sources over a short period of time or where a customer regularly transfers funds to one or more sources. For lower-risk situations that do not otherwise give rise to a business relationship, a three-month period for linking transactions might be appropriate, assuming this is not a regular occurrence.

Identification and verification of a beneficial owner

Regulations 3 & 5(b)

- 5.31 A beneficial owner is normally an individual who ultimately owns or controls the customer or on whose behalf a transaction or activity is being conducted. In respect of private individuals the customer himself is the beneficial owner, unless there are features of the transaction or surrounding circumstances that indicate otherwise. Therefore there is no requirement on institutions to make proactive searches for beneficial

owners in such cases, but they should make appropriate enquiries where it appears that the customer is not acting on his own behalf.

- 5.32 Where a customer who is a private individual is fronting for another individual who is the beneficial owner, the institution should obtain the same information about that beneficial owner as it would for a customer. For identifying beneficial owners of customers other than private individuals see paragraphs 5.104 onwards.

Regulation 5(a) & (b)

- 5.33 The *verification* requirements under the Regulations are, however, different as between a customer and a beneficial owner. The identity of a customer must be verified on the basis of documents, data or information obtained from a reliable and independent source. The obligation to verify the identity of a beneficial owner is for the institution to take risk-based and adequate measures so that it is satisfied that it knows who the beneficial owner is. It is up to each institution whether they make use of records of beneficial owners in the public domain (if any exist), ask their customers for relevant data or obtain the information otherwise. There is no specific requirement to have regard to particular types of evidence.

- 5.34 In lower-risk situations, therefore, it may be reasonable for the institution to be satisfied as to the beneficial owner's identity based on information supplied by the customer. This could include information provided by the customer (including trustees or other representatives whose identities have been verified) as to their identity, and confirmation that the beneficial owner is known to the customer. While this may be provided orally or in writing, any information received orally should be recorded in written form by the institution.

Regulation 3

- 5.35 The Regulations require that beneficial owners owning or controlling more than 25% of body corporates, partnerships or trusts are identified, and that risk-based and adequate measures are taken to verify their identities.

Regulation 3(3)(b)

- 5.36 In some trusts and similar arrangements, instead of being an individual, the beneficial owner is a class of persons who may benefit from the trust (see paragraphs 5.163). Where only a class of persons is required to be identified, it is sufficient for the institution to ascertain the name and the scope of the class, without identifying any members of the class.

Customers with whom institutions have a business relationship on 1st January 2009

Regulations 6(2)

- 5.37 Institutions must apply customer due diligence measures at appropriate times to its existing customers on a risk-sensitive basis. This guidance does not require the immediate application of customer due diligence measures to all existing customers after the 1st January 2009. The obligation to report suspicions of money laundering or terrorist financing, however, applies in respect of *all* the institution's customers.

- 5.38 As risk dictates, therefore, institutions must take steps to ensure that they hold appropriate information to demonstrate that they are satisfied that they know all their customers. Where the identity of an existing customer has already been verified to a previously applicable standard then, in the absence of circumstances indicating the contrary, the risk is likely to be low. A range of trigger events, such as an existing customer applying to open a new account or establish a new relationship, might prompt an institution to seek appropriate evidence.

- 5.39 Institutions that do not seriously address risks (including the risk that they have not confirmed the identity of existing customers) are exposing themselves to the possibility of action for breach of the Regulations.

- 5.40 An institution may hold considerable information in respect of a customer of some years standing. In some cases the issue may be more one of collating and assessing information already held than approaching customers for more identification data or information.

Acquisition of one AML/ATF regulated financial institution, or a portfolio of customers, by another

- 5.41 When an institution acquires the business and customers of another institution, either as a whole, or as a portfolio, it is not necessary for the identity of all existing customers to be re-verified, provided that:

- All underlying customer records are acquired with the business; or
- A warranty is given by the acquired institution or by the vendor where a portfolio of customers or business has been acquired, that the identities of its customers have been verified. It is, however, important that the acquiring institution's due diligence enquiries include some sample testing in order to confirm that the customer identification procedures previously followed by the acquired institution (or by the vendor, in relation to a portfolio) have been carried out in accordance with the requirements of the Regulations.

- 5.42 In the event that:

- The sample testing of the customer identification procedures previously undertaken shows that these have not been carried out to an appropriate standard; or
- The procedures cannot be checked; or
- The customer records are not accessible by the acquiring institution, verification of identity will need to be undertaken as soon as is practicable for all transferred customers who are not existing verified customers of the transferee, in line with the acquiring institution's risk-based approach, and the requirements for existing customers opening new accounts.

Nature and purpose of proposed business relationship

Regulation 5(c)

- 5.43 An institution must understand the purpose and intended nature of the business relationship or transaction. In some instances this will be self-evident, but in many cases the institution may have to obtain information in this regard.

- 5.44 Depending on the institution's risk assessment of the situation, information that might be relevant may include some or all of the following:

- Nature and details of the business/occupation/employment;
- Record of changes of address;
- The expected source and origin of the funds to be used in the relationship;
- Initial and on-going source(s) of wealth or income (particularly within a private banking or wealth management relationship);
- Copies of recent and current financial statements;
- The various relationships between signatories and with underlying beneficial owners; and
- The anticipated level and nature of the activity that is to be undertaken through the relationship.

Keeping information up to date

Regulation 7(2)(b)

- 5.45 Where information is held about customers, it must, as far as practicable, be kept up-to-date. Once the identity of a customer has been satisfactorily verified, there is no obligation to re-verify identity (unless doubts arise as to the veracity or adequacy of the evidence previously obtained for the purposes of customer identification); as risk dictates, however, institutions must take steps to ensure that they hold appropriate up-to-date information on their customers. A range of trigger events, such as an existing customer applying

to open a new account or establish a new relationship, might prompt an institution to seek appropriate evidence.

Characteristics and evidence of identity

- 5.46 The identity of an individual has a number of aspects: e.g. his/her given name (which of course may change), date of birth, place of birth. Other facts about an individual accumulate over time (the so-called electronic “footprint”): which will include family circumstances and addresses, employment and business career, contacts with the authorities or with other institutions and physical appearance.
- 5.47 The identity of a customer who is not a private individual is a combination of its constitution, its business, and its legal and ownership structure.
- 5.48 Evidence of identity can take a number of forms. In respect of individuals, much weight is placed on so-called ‘identity documents’, such as passports and photocard driving licences, and these are often the easiest way of being reasonably satisfied as to someone’s identity. It is, however, possible to be reasonably satisfied as to a customer’s identity based on other forms of confirmation, including, in appropriate circumstances, written assurances from persons or organisations that have dealt with the customer for some time.

Regulation 6(3)(a)

- 5.49 How much identity information or evidence to ask for, and what to verify, in order to be reasonably satisfied as to a customer’s identity, are matters for the judgement of the institution, which must be exercised on a risk-based approach, as set out in Chapter 4, taking into account factors such as:
- The nature of the product or service sought by the customer (and any other products or services to which they can migrate without further identity verification);
 - The nature and length of any existing or previous relationship between the customer and the institution;
 - The nature and extent of any assurances from other institutions that may be relied on; and
 - Whether the customer is physically present.
- 5.50 Evidence of identity can be in documentary or electronic form. An appropriate record of the steps taken and copies of, or references to, the evidence obtained to identify the customer, must be kept.

Documentary evidence

- 5.51 Documentation purporting to offer evidence of identity may emanate from a number of sources. These documents differ in their integrity, reliability and independence. Some are issued after due diligence on an individual’s identity has been undertaken; others are issued on request, without any such checks being carried out. There is a broad hierarchy of documents:
- Certain documents issued by government departments and agencies, or by a court; then
 - Certain documents issued by other public sector bodies or local authorities; then
 - Certain documents issued by regulated institutions in the financial services sector; then
 - Documents issued by other institutions subject to the Regulations, or to equivalent legislation; then
 - Documents issued by other organisations.
- 5.52 Institutions should recognise that some documents are more easily forged than others. If suspicions are raised in relation to any document offered, institutions should take whatever practical and proportionate steps are available to establish whether the document offered has been reported as lost or stolen.
- 5.53 In their procedures, therefore, institutions will in many situations need to be prepared to accept a range of documents, and they may wish also to employ electronic checks, either on their own or in tandem with documentary evidence.

Electronic evidence

- 5.54 Electronic data sources can provide a wide range of confirmatory material without involving the customer.
- 5.55 External electronic databases are accessible directly by institutions, or through independent third party organisations. The size of the electronic 'footprint' (see paragraph 5.46) in relation to the depth, breadth and quality of data, and the degree of corroboration of the data supplied by the customer, may provide a useful basis for an assessment of the degree of confidence in their identity.

Nature of electronic checks

- 5.56 A number of commercial agencies which access many data sources are accessible online by institutions, and may provide institutions with a composite and comprehensive level of electronic verification through a single interface. Such agencies use databases of both positive and negative information, and many also access high-risk alerts that utilise specific data sources to identify high-risk conditions, for example, known identity frauds or inclusion on a sanctions list. Some of these sources are, however, only available to closed user groups.
- 5.57 Positive information (relating to full name, current address, date of birth) can prove that an individual exists, but some can offer a higher degree of confidence than others. Such information should include data from more robust sources - where an individual has to prove their identity, or address, in some way in order to be included, as opposed to others, where no such proof is required.
- 5.58 Negative information includes lists of individuals known to have committed fraud, including identity fraud, and registers of deceased persons. Checking against such information may be necessary to mitigate against impersonation fraud.
- 5.59 For an electronic check to provide satisfactory evidence of identity on its own, it must use data from multiple sources and across time, or incorporate qualitative checks that assess the strength of the information supplied. An electronic check that accesses data from a single source (e.g. a single check against the Parliamentary Register) is not normally enough on its own to verify identity.

Criteria for use of an electronic data provider

- 5.60 Before using a commercial agency for electronic verification, institutions should be satisfied that information supplied by the data provider is considered to be sufficiently extensive, reliable and accurate. This judgement may be assisted by considering whether the provider meets all the following criteria:
- It uses a range of positive information sources that can be called upon to link an applicant to both current and previous circumstances;
 - It accesses negative information sources, such as databases relating to identity fraud and deceased persons;
 - It accesses a wide range of alert data sources; and
 - It has transparent processes that enable the institution to know what checks were carried out, what the results of these checks were, and what they mean in terms of how much certainty they give as to the identity of the subject.
- 5.61 In addition, a commercial agency should have processes that allow the enquirer to capture and store the information they used to verify an identity.

Shell banks and anonymous accounts

Regulation 13 (1), (2) & (5)

- 5.62 Institutions must not enter into, or continue, a correspondent banking relationship with a shell bank. Institutions must take appropriate measures to ensure that they do not enter into or continue a correspondent banking relationship with a bank that is known to permit its accounts to be used by a shell

bank. A shell bank is an entity incorporated in a jurisdiction where it has no physical presence involving meaningful decision-making and management, and which is unaffiliated with a regulated financial group.

Regulation 13 (3) & (4)

- 5.63 Institutions carrying on business in Bermuda must not set up an anonymous account or an anonymous passbook for any new or existing customer. As soon as possible after the 1st January 2009, all institutions carrying on business in Bermuda must apply customer due diligence measures to all existing anonymous accounts and passbooks, and in any event before such accounts or passbooks are used in any way.
- 5.64 Institutions should pay special attention to any money laundering or terrorist financing threat that may arise from products or transactions that may favour anonymity and take measures, if needed, to prevent their use for money laundering or terrorist financing purposes.

Private individuals

General

- 5.65 Paragraphs 5.67 to 5.83 refer to the standard identification requirement for customers who are private individuals; paragraphs 5.84 to 5.103 provide further guidance on steps that may be applied as part of a risk based approach.
- 5.66 Depending on the circumstances relating to the customer, the product and the nature and purpose of the proposed relationship, institutions may also need to apply the following guidance to identifying and verifying the identity of beneficial owners, and to other relevant individuals associated with the relationship or transaction (but see paragraphs 5.33 & 5.34).

Obtain standard evidence: Identification

- 5.67 The institution should obtain the following information in relation to the private individual;
- Full name;
 - Residential address; and
 - Date of birth.

Verification

- 5.68 Verification of the information obtained must be based on reliable and independent sources – which might either be a document or documents produced by the customer, or electronically by the institution, or by a combination of both. Where business is conducted face-to-face, institutions should see originals of any documents involved in the verification. Customers should be discouraged from sending original valuable documents by post.

Documentary verification

- 5.69 If documentary evidence of an individual's identity is to provide a high level of confidence, it will typically have been issued by a government department or agency, or by a court, because there is a greater likelihood that the authorities will have checked the existence and characteristics of the persons concerned. In cases where such documentary evidence of identity may not be available to an individual, other evidence of identity may give the institution reasonable confidence in the customer's identity, although the institution should weigh these against the risks involved.
- 5.70 Non-government issued documentary evidence complementing identity should normally only be accepted if it originates from a public sector body or another institution, or is supplemented by knowledge that the institution has of the person or entity, which it has documented.
- 5.71 If identity is to be verified from documents, this should be based on:

Either a government issued document which incorporates:

- The customer's full name and photograph, and
 - Either his residential address; or
 - Date of birth.

5.72 Government issued documents with a photograph include:

- Valid passport;
- Valid driving licence.

or a government issued document (without a photograph) which incorporates the customer's full name, *supported by* a second document, either government issued or issued by a judicial authority, a public sector body or authority, a utility company, or another institution in Bermuda or in an equivalent jurisdiction, which incorporates:

- The customer's full name, and
 - Either his residential address; or
 - Date of birth.

5.73 Government issued documents without a photograph include:

- Birth Certificate.

5.74 Other documents include:

- Instrument of a court appointment (such as liquidator, or grant of probate);
- Current land tax demand letter, or statement;
- Current bank statements, or credit/debit card statements, issued by an institution in Bermuda or an institution in an equivalent jurisdiction outside Bermuda (but not ones printed off the internet); and
- Utility bills (but not ones printed off the internet).

5.75 The examples of other documents are intended to support a customer's address, and so it is likely that they will have been delivered to the customer through the post, rather than being accessed by him across the internet.

5.76 Where a member of the institution's staff has visited the customer at his home address, a record of this visit may constitute evidence corroborating that the individual lives at this address, (i.e. as a second document).

5.77 In practical terms, this means that, for face-to-face verification, production of a valid passport or photocard driving licence should enable most individuals to meet the identification requirement for AML/ATF purposes. For customers who cannot provide the standard evidence, other documents may be appropriate (see paragraphs 5.97 to 5.101).

5.78 Some consideration should be given as to whether the documents relied upon are forged. In addition, if they are in a foreign language, appropriate steps should be taken to be reasonably satisfied that the documents in fact provide evidence of the customer's identity. Commercial software is also available that checks the algorithms used to generate passport numbers. This can be used to check the validity of passports of any country that issues machine-readable passports.

Electronic verification

5.79 If identity is verified electronically, this should be by the institution, using as its basis the customer's full name, address and date of birth, carrying out electronic checks either direct or through a supplier which meets the criteria in paragraphs 5.60 & 5.61, providing a reasonable assurance that the customer is who he says he is.

- 5.80 As well as requiring a commercial agency used for electronic verification to meet the criteria set out in paragraphs 5.60 & 5.61, it is important that the process of electronic verification meets a standard level of confirmation before it can be relied on. The standard level of confirmation, in circumstances that do not give rise to concern or uncertainty, is:
- One match on an individual's full name and current address; and
 - A second match on an individual's full name and either his current address or his date of birth.
- 5.81 Commercial agencies that provide electronic verification use various methods of displaying results - for example, by the number of documents checked, or through scoring mechanisms. Institutions should ensure that they understand the basis of the system they use, in order to be satisfied that the sources of the underlying data reflect the guidance in paragraphs 5.56 to 5.59, and cumulatively meet the standard level of confirmation set out above.
- 5.82 To mitigate the risk of impersonation fraud, institutions should either verify with the customer additional aspects of his identity which are held electronically, or follow the guidance in paragraph 5.83.

Mitigation of impersonation risk

- 5.83 Where identity is verified electronically, or copy documents are used, an institution should apply an additional verification check to manage the risk of impersonation fraud. The additional check may consist of robust anti-fraud checks that the institution routinely undertakes as part of its existing procedures, or may include:
- Requiring the first payment to be carried out through an account in the customer's name with a Bermuda institution or one from an equivalent jurisdiction;
 - Verifying additional aspects of the customer's identity, or of his electronic 'footprint' (see paragraph 5.46);
 - Telephone contact with the customer prior to opening the account on a home or business number which has been verified (electronically or otherwise), or a "welcome call" to the customer before transactions are permitted, using it to verify additional aspects of personal identity information that have been previously provided during the setting up of the account;
 - Communicating with the customer at an address that has been verified (such communication may take the form of a direct mailing of account opening documentation to him, which, in full or in part, might be required to be returned completed or acknowledged without alteration);
 - Internet sign-on following verification procedures where the customer uses security codes, tokens or other passwords which have been set up during account opening and provided by mail (or secure delivery) to the named individual at an independently verified address;
 - Other card or account activation procedures; and
 - Requiring copy documents to be certified by an appropriate person.

Variation from the standard

- 5.84 The standard identification requirement (for documentary or electronic approaches) is likely to be sufficient for most situations. If, however, the customer, and/or the product or delivery channel, is assessed to present a higher money laundering or terrorist financing risk – whether because of the nature of the customer, or his business, or its location, or because of the product features available – the institution will need to decide whether it should require additional identity information to be provided, and/or whether to verify additional aspects of identity.
- 5.85 Where the result of the standard verification check gives rise to concern or uncertainty over identity, or other risk considerations apply, so the number of matches that will be required to be reasonably satisfied as to the individual's identity will increase.
- 5.86 For higher-risk customers, the need to have additional information needs to be balanced against the possibility of instituting enhanced monitoring (see paragraphs 5.216 to 244 and 5.283 to 5.303).

Executors and personal representatives

Regulation 3(8)

- 5.87 In the case of an estate of a deceased person, during the course of administration the beneficial owner is the executor or administrator of the deceased person.
- 5.88 In circumstances where an account is opened or taken over by executors or administrators for the purpose of winding up the estate of a deceased person, institutions may accept the court documents granting probate or letters of administration as evidence of identity of those personal representatives. Lawyers and accountants acting in the course of their business as independent professionals, who are not named as executors/administrators, can be verified by reference to their practicing certificates, or to an appropriate professional register.

Attorneys

- 5.89 When a person deals with assets under a power of attorney, that person is also a customer of the institution. Consequently, the identity of holders of powers of attorney should be verified.
- 5.90 Where the donor of a power of attorney has capacity, and therefore has control, he remains the owner of the funds, and is the customer. Other than where he is an existing customer of the institution, therefore, his identity must be verified. In many cases, these customers may not possess the standard identity documents referred to in (paragraphs 5.71), and institutions may have to accept other documents.
- 5.91 In circumstances where he has lost capacity, the donor no longer has control of the property, but his identity should be verified as the beneficial owner.

Source of funds as evidence

- 5.92 Under certain conditions, where the money laundering or terrorist financing risk in a product is considered to be at its lowest, a payment drawn on an account with a Bermuda institution, or one from an equivalent jurisdiction, and which is in the sole or joint name of the customer, may satisfy the standard identification requirement. Whilst the payment may be made between accounts with institutions or by cheque or debit card, the accepting institution must be able to confirm that the payment (by whatever method) is from an account held with an institution in the sole or joint name(s) of the customer.
- 5.93 Whilst it is immaterial whether the transaction is effected remotely or face-to-face, each type of relationship or transaction that is entered into must be considered before determining that it is appropriate to rely on this method of verification. Institutions will need to be able to demonstrate why they considered it to be reasonable to have regard to the source of funds as evidence in a particular instance.
- 5.94 One of the restrictions that will apply to a product that qualifies for using the source of funds as evidence will be an inability to make payments direct to, or to receive payments direct from, third parties. If, subsequent to using the source of funds to verify the customer's identity, the institution decides to allow such a payment or receipt to proceed, it should verify the identity of the third party. A further restriction would be that cash withdrawals should not be permitted, other than by the customers themselves, on a face-to-face basis where identity can be confirmed.
- 5.95 If an institution proposing to rely on the source of funds has reasonable grounds for believing that the identity of the customer has not been verified by the institution on which the payment has been drawn, it should not permit the source of funds to be used as evidence, and should verify the customer's identity in line with the appropriate standard requirement.
- 5.96 If an institution has reason to suspect the motives behind a particular transaction, or believes that the business is being structured to avoid the standard identification requirement, it should not permit the use of the source of funds as evidence to identify the customer.

Customers who cannot provide the standard evidence

- 5.97 Some customers may not be able to produce identification information equivalent to the standard. Such cases may include, for example, some low-income customers in rented accommodation, customers with a legal, mental or physical inability to manage their affairs, individuals dependent on the care of others, dependant spouses/partners or minors, students and prison inmates. The institution will therefore need an approach that compensates for the difficulties that such customers may face in providing the standard evidence of identity.
- 5.98 Institutions are encouraged to adopt a broad view of financial exclusion, in terms of ensuring that, where people cannot reasonably be expected to produce standard evidence of identity, they are not unreasonably denied access to financial services.
- 5.99 Institutions offering financial services directed at the financially aware may wish to consider whether any apparent inability to produce standard levels of identification evidence is consistent with the targeted market for these products.
- 5.100 As a first step, before concluding that a customer cannot produce evidence of identity, institutions will have established that the guidance on initial identity checks for private individuals set out in paragraphs 5.67 to 5.78 cannot reasonably be applied.
- 5.101 Where an institution concludes that an individual customer cannot reasonably meet the standard identification requirement, it may accept as identification evidence a letter or statement from an appropriate person who knows the individual, that indicates that the person is who he says he is.

Students and young people

- 5.102 When opening accounts for students or other young people, the standard identification requirement should be followed as far as possible (see paragraphs 5.67 to 5.78). In practice, it is likely that many students, and other young people, will have a passport, and possibly a driving licence. Where the standard requirement would not be relevant, however, or where the customer cannot satisfactorily meet this, other evidence could be obtained by obtaining appropriate confirmation(s) from the applicant's workplace, school, college or university. Any confirmatory letter should be on appropriately headed notepaper; in assessing the strength of such confirmation, institutions should have regard to the period of existence of the educational or other institution involved, and whether it is subject to some form of regulatory oversight.
- 5.103 Often, a business relationship in respect of a minor will be established by a family member or guardian. In cases where the adult opening the account or establishing the relationship does not already have an existing relationship with the institution, the identity of that adult should be verified and, in addition, the institution should see one of the following in the name of the child:
- Birth certificate; or
 - Passport.

Customers other than private individuals

- 5.104 Depending on the nature of the entity, a relationship or transaction with a customer who is not a private individual may be entered into in the customer's own name, or in that of specific individuals or other entities on its behalf. Beneficial ownership may, however, rest with others, either because the legal owner is acting for the beneficial owner, or because there is a legal obligation for the ownership to be registered in a particular way.

Regulation 5(b)

- 5.105 In deciding who the beneficial owner is in relation to a customer who is not a private individual, the institution's objective must be to know who has ownership or control over the funds which form or

otherwise relate to the relationship, and/or form the controlling mind and/or management of any legal entity involved in the funds. Verifying the identity of the beneficial owner(s) should be carried out on a risk-based approach, following the guidance in paragraphs 5.30 & 5.34, and should take account of the number of individuals, the nature and distribution of their interests in the entity and the nature and extent of any business, contractual or family relationship between them.

- 5.106 Certain other information about the entity should be obtained as a standard requirement. Thereafter, on the basis of the money laundering/terrorist financing risk assessed in the customer/product/delivery channel combination, an institution should decide the extent to which the identity of the entity should be verified. The institution should also decide what additional information in respect of the entity and, potentially, some of the individuals behind it, should be obtained (see paragraphs 5.216 to 5.24).
- 5.107 Many entities, both in Bermuda and elsewhere, operate internet websites, which contain information about the entity. Institutions should bear in mind that this information, although helpful in providing much of the material that an institution might need in relation to the company, its directors and business, is not independently verified before being made publicly available in this way.
- 5.108 This section provides guidance on verifying the identity of a range of non-personal entities, as follows:
- Corporates;
 - Pension schemes;
 - Charities, church bodies and places of worship;
 - Registered charities;
 - Independent schools and colleges;
 - Other trusts, foundations and similar entities;
 - Other entities that are subject to the Regulations (or equivalent);
 - Partnerships and unincorporated businesses; and
 - Clubs and societies.

Corporates

- 5.109 Corporate customers may be publicly accountable in several ways. Some public companies are listed on stock exchanges or other regulated markets, and are subject to market regulation and to a high level of public disclosure in relation to their ownership and business activities. Other public companies are unlisted, but are still subject to a high level of disclosure through public filing obligations. Private companies are not generally subject to the same level of disclosure, although they may often have public filing obligations. In their verification processes, institutions should take account of the availability of public information in respect of different types of company.

Regulation 16(2)(a)

- 5.110 The structure, ownership, purpose and activities of many corporates will be clear and understandable. Corporate customers can use complex ownership structures, which can increase the steps that need to be taken to be reasonably satisfied as to their identities; this does not necessarily indicate money laundering or terrorist financing. The use of complex structures without an obvious legitimate commercial purpose may, however, give rise to concern and increase the risk of money laundering or terrorist financing.
- 5.111 Control over companies may be exercised through a direct shareholding or through intermediate holding companies. Control may also rest with those who have power to manage funds or transactions without requiring specific authority to do so, and who would be in a position to override internal procedures and control mechanisms. Institutions should make an evaluation of the effective distribution of control in each case. What constitutes control for this purpose will depend on the nature of the company, the distribution of shareholdings, and the nature and extent of any business or family connections between the beneficial owners.

Regulation 5(c)

- 5.112 To the extent consistent with the risk assessment carried out in accordance with the guidance in Chapter 4, the institution should ensure that it fully understands the company's legal form, structure and ownership, and must obtain sufficient additional information on the nature of the company's business, and the reasons for seeking the product or service.

Regulation 3(1)

- 5.113 In the case of a body corporate the beneficial owner includes any individual who:
- As regards any body other than a company listed on an appointed stock exchange, ultimately owns or controls (whether through direct or indirect ownership or control, including through bearer share holdings) more than 25% of the shares or voting rights in the body; or
 - As regards any body corporate, otherwise exercises control over the management of the body.
- 5.114 Directors of a body corporate do not fall under the definition of beneficial owner, as in the capacity of director they do not have an ownership interest in the body, nor do they control the voting rights in the body, nor do they exercise control over management in the sense of being able to control the composition and/or voting of the board of directors.
- 5.115 Paragraphs 5.116 to 5.130 refer to the standard evidence for corporate customers, and paragraphs 5.131 to 5.135 provide further supplementary guidance on steps that may be applied as part of a risk-based approach.

Obtain standard evidence

- 5.116 The institution should obtain the following in relation to the corporate concerned:
- Full name;
 - Registered number (if applicable);
 - Registered office in country of incorporation (if applicable);
 - Business address and, additionally, for private or unlisted companies;
 - Names of all directors (or equivalent); and
 - Names of individuals who own or control over 25% of its shares or voting rights.
- 5.117 The institution should verify the existence of the corporate from:
- either* confirmation of the company's listing on an appointed stock exchange *or* a search of the relevant company registry *or* a copy of the company's Certificate of Incorporation
- 5.118 Institutions should take appropriate steps to be reasonably satisfied that the person the institution is dealing with is properly authorised by the customer.
- 5.119 Some consideration should be given as to whether documents relied upon are forged. In addition, if they are in a foreign language, appropriate steps should be taken to be reasonably satisfied that the documents in fact provide evidence of the customer's identity.

Companies listed on an appointed stock exchange

- 5.120 Corporate customers whose securities are admitted to trading on an appointed stock exchange are publicly owned and generally accountable.

Regulation 10(3)

5.121 Where the institution has satisfied itself that the customer is:

- A company which is listed on an appointed stock exchange that is subject to disclosure obligations; or
- A majority-owned and consolidated subsidiary of such a listed company

simplified due diligence may be applied.

Regulation 2(1)

5.122 If the market is outside Bermuda, but is one which subjects companies whose securities are admitted to trading to disclosure obligations which are contained in international standards and are equivalent to the specified disclosure obligation in Bermuda, similar treatment is permitted. For companies listed outside Bermuda on markets that do not qualify for SDD, the standard verification requirement for private and unlisted companies should be applied.

Private and unlisted companies

5.123 Unlike publicly quoted companies, the activities of private or unlisted companies are often carried out for the profit/benefit of a small and defined group of individuals or entities. Such companies are also subject to a lower level of public disclosure than public companies. In general, however, the structure, ownership, purposes and activities of many private companies will be clear and understandable.

5.124 Where private companies are well-known, reputable organisations, with long histories in their industries and substantial public information about them, the standard evidence may well be sufficient to meet the institution's obligations.

5.125 A company registry search will confirm that the applicant company has not been, or is not in the process of being, dissolved, struck off or wound up. In the case of non-Bermuda companies, institutions should, as far as practicable, make similar search enquiries of the registry in the country of incorporation of the applicant for business.

5.126 Standards of control over the issue of documentation from company registries vary between different countries. Attention should be paid to the jurisdiction the documents originate from and the background against which they are produced.

5.127 Whenever faced with less transparency, less of an industry profile, or less independent means of verification of the client entity, institutions should consider the money laundering or terrorist financing risk presented by the entity, and therefore the extent to which, in addition to the standard evidence, they should verify the identities of other shareholders and/or controllers. It is important to know and understand any associations the entity may have with other jurisdictions (headquarters, operating facilities, branches, subsidiaries, etc) and the individuals who may influence its operations (political connections, etc). A visit to the place of business may be helpful to confirm the existence and activities of the entity.

Directors

5.128 Following the institutions assessment of the money laundering or terrorist financing risk presented by the company, it may decide to verify the identity of one or more directors, as appropriate, in accordance with the guidance for private individuals (paragraphs 5.65 to 5.103). In that event, verification is likely to be appropriate for those who have authority to operate an account or to give the institution instructions concerning the use or transfer of funds or assets, but might be waived for other directors. Institutions may, of course, already be required to identify a particular director as a beneficial owner if the director owns or controls more than 25% of the company's shares or voting rights (see paragraph 5.113).

Beneficial owners

Regulation 3(1)&5(b)

- 5.129 As part of the standard evidence, the institution will know the names of all individual beneficial owners owning or controlling more than 25% of the company's shares or voting rights, even where these interests are held indirectly. Following the institution's assessment of the money laundering or terrorist financing risk presented by the customer, the institution must take risk-based and adequate measures to verify the identity of those individuals (see paragraphs 5.33 & 5.34).

Signatories

- 5.130 For operational purposes, the institution is likely to have a list of those authorised to give instructions for the movement of funds or assets, along with an appropriate instrument authorising one or more directors (or equivalent) to give the institution such instructions. The identities of individual signatories need only be verified on a risk-based approach.

Variation from the standard

Regulation 11(1)(b)

- 5.131 The standard evidence is likely to be sufficient for most corporate customers. If, however, the customer, or the product or delivery channel, is assessed to present a higher money laundering or terrorist financing risk – whether because of the nature of the customer, its business or its location, or because of the product features available – the institution must, on a risk-sensitive basis, apply enhanced due diligence measures. For example, the institution will need to decide whether it should require additional identity information to be provided and/or verified (see paragraphs 5.245 to 5.303).
- 5.132 Higher risk corporate customers may also be, among others, smaller and more opaque entities, with little or no industry profile and those in less transparent jurisdictions, taking account of issues such as their size, industry profile, industry risk.

Regulation 11(1)(b) & 11(4)

- 5.133 Where an entity is known to be linked to a PEP, or to a jurisdiction assessed as carrying a higher money laundering/terrorist financing risk, it is likely that this will put the entity into a higher-risk category, and that enhanced due diligence measures must therefore be applied (see paragraphs 5.216 to 5.244 and 5.283 to 5.303).

Bearer shares

- 5.134 Extra care must be taken in the case of companies with capital in the form of bearer shares, because in such cases it is often difficult to identify the beneficial owner(s). Companies that issue bearer shares are frequently incorporated in high-risk jurisdictions. Institutions should adopt procedures to establish the identities of the holders and material beneficial owners of such shares and to ensure that they are notified whenever there is a change of holder and/or beneficial owner.
- 5.135 As a minimum, these procedures should require an institution to obtain an undertaking in writing from the beneficial owner which states that immediate notification will be given to the institution if the shares are transferred to another party. Depending on its risk assessment of the client, the institution may consider it appropriate to have this undertaking certified or even to require that the shares be held by a named custodian, with an undertaking from that custodian that the institution will be notified of any changes to records relating to these shares and the custodian.

Pension schemes

- 5.136 Bermuda pension schemes can take a number of legal forms. Some may be companies limited by guarantee; some may take the form of trusts; others may be unincorporated associations.

Regulation 10(6)(c)

- 5.137 In respect of a pension, superannuation or similar scheme which provides retirement benefits for employees, where contributions are made by an employer or by way of deduction from an employee's wages and the scheme rules do not permit the assignment of a member's interest under the scheme, simplified due diligence may be applied (see paragraphs 5.209 to 5.215).
- 5.138 For such a scheme, therefore, the institution need only satisfy itself that the customer qualifies for simplified due diligence in this way. In other cases, a pension scheme should be treated for AML/ATF purposes, (and standard evidence obtained), according to its legal form.

Obtain standard evidence

Signatories

- 5.139 For operational purposes, the institution is likely to have a list of those authorised to give instructions for the movement of funds or assets, along with an appropriate instrument authorising one or more directors (or equivalent) to give the institution such instructions. The identities of individual signatories need only be verified on a risk-based approach.

Variation from the standard

- 5.140 The identity of the principal employer should be verified in accordance with the guidance given for companies in paragraphs 5.109 to 5.135 and the source of funding recorded to ensure that a complete audit trail exists if the employer is wound up.

Payment of benefits

- 5.141 Any payment of benefits by, or on behalf of, the trustees of an occupational pension scheme will not require verification of identity of the recipient.
- 5.142 Where individual members of an occupational pension scheme are to be given personal investment advice, their identities must be verified. However, where the identity of the trustees and principal employer have been satisfactorily verified (and the information is still current), it may be appropriate for the employer to provide confirmation of identities of individual employees.

Charities, church bodies and places of worship

- 5.143 Charities have their status because of their purposes, and can take a number of legal forms. Some may be companies limited by guarantee, or incorporated by an Act of Parliament; some may take the form of trusts; others may be unincorporated associations.
- 5.144 If the charity is an incorporated entity (or otherwise has legal personality); institutions should verify its identity following the guidance in paragraphs commencing at 5.109. The charity itself is the institution's customer, for practical purposes represented by the Directors who give instruction to the institution.
- 5.145 If the charity takes the form of a trust, it has no legal personality and its trustees have control and management over its affairs. Those trustees who enter into the business relationship with the institution, in their capacity as trustees of that particular charitable trust, are the institution's customers, on whom the institution must carry out full customer due diligence measures. (see paragraphs commencing at 5.160)
- 5.146 If the charity takes the form of an unincorporated association, it also has no legal personality. Its officers, or members of its governing body, are then the institution's customers, on whom the institution must carry out full customer due diligence measures. (see paragraphs commencing at 5.200)
- 5.147 Any trustees of a charitable trust who are not the institution's customers will be beneficial owners, because they exercise control over the charity's property. In exceptional cases, another individual may exercise

control. Examples include a receiver appointed to manage the affairs of the charity, or a settlor who retains significant powers over the trust property.

- 5.148 For the vast majority of charities either there will be no individual who is a beneficial owner (apart from the trustees) within the meaning of the Regulations. At most a class of persons who stand to benefit from the charity's objects must be identified. These persons will be self-evident from a review of the charity's objects in its constitution or the extract from the register of charitable organisations maintained by the Registrar.
- 5.149 Examples of charities where classes of persons can be identified include charities that relieve poverty, famine or homelessness, educate individuals or alleviate sickness, disability or age. In these cases, a broad description of the class of persons who stand to benefit is sufficient as long as the institution understands who the persons are who benefit.
- 5.150 In other charities, no one benefits directly from the charity's objects. Examples include charities for the benefit of animals, wildlife or flora, or the conservation or preservation of buildings, habitats or environment.

Obtain standard evidence

- 5.151 The institution should obtain the following in relation to the charity or church body:
- Full name and address;
 - Nature of body's activities and objects;
 - Names of all trustees (or equivalent); and
 - Names or classes of beneficiaries.
- 5.152 The existence of the charity can be verified from a number of different sources, depending on whether the charity is registered or not, a place of worship or an independent school or college.

Registered charities – Bermuda

- 5.153 The Registrar is required to maintain register of charities in Bermuda. Every registered charitable organisation is required to file annual accounts, within six months from the end of the financial year, with the Registrar. Accounts filed with the Registrar are available for inspection by members of the public during normal working hours. Institutions should be aware that simply being registered is not in itself a guarantee of the bona fides of an organisation, although it does indicate that it is subject to some on-going regulation.

Independent schools and colleges

- 5.154 Where an independent school or college is a registered charity, it should be treated in accordance with the guidance for charities. Any such body which is not registered as a charity should be treated in accordance with the guidance for private companies in paragraphs 5.123 to 5.130.
- 5.155 Institutions should take appropriate steps to be reasonably satisfied that the person the institution is dealing with is properly authorised by the customer.

Variation from the standard

- 5.156 The identities of unregistered charities or church bodies, whether in Bermuda or elsewhere, cannot be verified by reference to registers maintained by independent bodies. Applications from, or on behalf of, unregistered charities should therefore be dealt with in accordance with the procedures for private companies set out in paragraphs 5.123 to 5.130, for trusts, as set out in paragraphs 5.160 to 5.182, or for clubs and societies, as set out in paragraphs 5.200 to 5.208. Institutions should take particular note of those paragraphs addressing customers where the money laundering or terrorist financing risk is greater in relation to particular customers, and if it should be followed in these circumstances.

- 5.157 In assessing the risks presented by different charities, an institution might need to make appropriate distinction between those with a limited geographical remit, and those with unlimited geographical scope, such as medical and emergency relief charities.
- 5.158 If they have a defined area of benefit, charities are only able to expend their funds within that defined area. If this area is an overseas country or jurisdiction, the charity can quite properly be transferring funds to that country or jurisdiction. It would be less clear why the organisation should be transferring funds to a third country (which may, within the general context of the institution's risk assessment have a lower profile) and this would therefore be unusual. Such activity would lead to the charity being regarded as higher-risk.
- 5.159 Non-profit organisations have been known to be abused, to divert funds to terrorist financing and other criminal activities. FATF published a paper [International Best Practices: Combating the abuse of non-profit organisations - Special Recommendation VIII](#) in October 2002.

Other trusts, foundations and similar entities

- 5.160 There is a wide variety of trusts, ranging from large, nationally and internationally active organisations subject to a high degree of public interest and quasi-accountability, through trusts set up under testamentary arrangements, to small, local trusts funded by small, individual donations from local communities, serving local needs. It is important, in putting proportionate AML/ATF processes into place, and in carrying out their risk assessments, that institutions take account of the different money laundering or terrorist financing risks that trusts of different sizes, areas of activity and nature of business being conducted, present.
- 5.161 For trusts or foundations that have no legal personality, those trustees (or equivalent) who enter into the business relationship with the institution, in their capacity as trustees of the particular trust or foundation, are the institution's customers on whom the institution must carry out full customer due diligence measures. Following a risk-based approach, in the case of a large, well known and accountable organization, institutions may limit the trustees considered customers to those who give instructions to the institution. Other trustees will be verified as beneficial owners, following the guidance in paragraphs 5.33 & 5.34.
- 5.162 Most trusts are not separate legal persons, and for AML/ATF purposes should be identified as described in paragraphs 5.168 & 5.169.
- 5.163 The beneficial owner of a trust is defined by reference to three categories of individual:

Regulation 3(3)&(4)

- Any individual who is entitled to a specified interest (that is, a vested, not a contingent, interest) in at least 25% of the capital of the trust property;
- As respects any trust other than one which is set up or operates entirely for the benefit of individuals with such specified interests, the class of persons in whose main interest the trust is set up or operates; and
- Any individual who has control over the trust.

Regulation 3(4)

- 5.164 The trustees of a trust will be beneficial owners, as they will exercise control over the trust property. In exceptional cases, another individual may exercise control, such as a trust protector, or a settlor who retains significant powers over the trust property.
- 5.165 For the vast majority of trusts, either there will be clearly identified beneficiaries (who are beneficial owners within the meaning of the Regulations), or a class of beneficiaries. These persons will be self-evident from a review of the trust's constitution.

5.166 In some trusts, no individuals may benefit directly; examples include trusts for the benefit of animals, wildlife or flora, or the conservation or preservation of buildings, habitats or environment.

Regulation 3(6)

5.167 In the case of a legal arrangement that is not a trust, the beneficial owner means:

- Where the individuals who benefit from the entity or arrangement have been determined, any individual who benefits from at least 25% of the property of the entity or arrangement;
- Where the individuals who benefit from the entity or arrangement have yet to be determined, the class of persons in whose main interest the entity or arrangement is set up or operates; or
- Any individual who exercises control over at least 25% of the property of the entity or arrangement.

Obtain standard evidence

5.168 In respect of trusts, the institution should obtain the following information:

- Full name of the trust;
- Nature and purpose of the trust (e.g. discretionary, testamentary, bare);
- Country of establishment;
- Names of all trustees;
- Names of any beneficial owners; and
- Name and address of any protector or controller.

5.169 The identity of the trust must be verified using reliable and independent documents, data or information. This may require sight of relevant extracts from the trust deed. The institution must take measures to understand the ownership and control structure of the customer.

5.170 Institutions should take appropriate steps to be reasonably satisfied that the person the institution is dealing with is properly authorised by the customer. Some consideration should be given as to whether documents relied upon are forged. In addition, if they are in a foreign language, appropriate steps should be taken to be reasonably satisfied that the documents in fact provide evidence of the customer's identity.

Beneficial owners

5.171 The institution must verify the identities of the trustees (or equivalent) as beneficial owners, if not already identified as customers of the institution. The identities of other beneficial owners, either individuals or a class, as appropriate, must also be verified (see paragraphs 5.33 & 5.34).

5.172 Where a trustee is itself an institution (or a nominee company owned and controlled by an institution), or a company listed on an appointed stock exchange, the identification and verification procedures that should be carried out should reflect the standard approach for such an entity.

Variation from the standard

5.173 Institutions should make appropriate distinction between those trusts that serve a limited purpose (such as inheritance tax planning) or have a limited range of activities and those where the activities and connections are more sophisticated, or are geographically based and/or with financial links to other countries.

5.174 For situations presenting a lower money laundering or terrorist financing risk, the standard evidence will be sufficient. However, less transparent and more complex structures, with numerous layers, may pose a higher money laundering or terrorist financing risk.

5.175 Where a situation is assessed as carrying a higher-risk of money laundering or terrorist financing, the institution may need to carry out a higher level of verification. Information that might be appropriate to ascertain for higher-risk situations includes:

- Donor/settlor/grantor of the funds (except where there are large numbers of small donors);
- Domicile of business/activity;
- Nature of business/activity; and
- Location of business/activity (operating address).

5.176 Following its assessment of the money laundering risk presented by the trust, the institution may decide to verify the identity of the settlor(s).

Non-Bermuda trusts and foundations

5.177 The guidance in paragraphs 5.160 to 5.176 applies equally to Bermuda based trusts and non-Bermuda based trusts. On a risk-based approach, an institution will need to consider whether the geographical location of the trust gives rise to additional concerns, and if so, what they should do.

5.178 A foundation (“Stiftung”) is described in the FATF October 2006 *Report on the Misuse of Corporate Vehicles* as follows:

5.179 “A foundation (based on the Roman law *universitas rerum*) is the civil law equivalent to a common law trust in that it may be used for similar purposes. A foundation traditionally requires property dedicated to a particular purpose. Typically the income derived from the principal assets (as opposed to the assets themselves) is used to fulfill the statutory purpose. A foundation is a legal entity and as such may engage in and conduct business. A foundation is controlled by a board of directors and has no owners. In most jurisdictions a foundation’s purpose must be public. However there are jurisdictions in which foundations may be created for private purposes. Normally, foundations are highly regulated and transparent.”

5.180 Foundations feature in a number of civil law jurisdictions including, notably, Liechtenstein and Panama. The term is also used in the UK and USA in a looser sense, usually to refer to a charitable organisation of some sort.

5.181 The nature of a civil law foundation should normally be well understood by institutions, or their subsidiaries or branches, operating in the jurisdiction under whose laws the foundation has been set up. Where a foundation seeks banking or other financial services outside its home jurisdiction, institutions will need to be satisfied that there are legitimate reasons for doing so and to establish the statutory requirements within the specific home jurisdiction for setting up a foundation. So far as possible, comparable information should be obtained as indicated in paragraph 5.168 for trusts, including the identity of the founder and beneficiaries (who may include the founder), whose identity should be verified as necessary on similar risk-based principles.

5.182 Whilst institutions may conclude on the basis of their due diligence that the request for facilities is acceptable, they should bear in mind that terms like ‘foundation’, ‘stiftung’, ‘anstalt’ are liable to be hijacked by prime bank instrument fraudsters to add spurious credibility to bogus investment schemes.

Other Entities that are subject to the Regulations (or equivalent)

5.183 Customers which are subject to the Regulations or equivalent, but which are not regulated in Bermuda or an equivalent jurisdiction as an institution, should be treated, for AML/ATF purposes, according to their legal form: for example, as private companies, in accordance with the guidance set out in paragraphs 5.123 to 5.130; or if partnerships, by confirming their regulated status through reference to the current membership directory of the relevant professional association (for example, law society or accountancy body). However, when professional individuals are acting in their personal capacity, for example, as trustees, their identity should normally be verified as for any other private individual.

5.184 Institutions should take appropriate steps to be reasonably satisfied that the person it is dealing with is properly authorised by the customer.

- 5.185 Some consideration should be given as to whether documents relied upon are forged. In addition, if they are in a foreign language, appropriate steps should be taken to be reasonably satisfied that the documents in fact provide evidence of the customer's identity.

Regulation 10(4)

- 5.186 Independent professionals that are subject to the Regulations, or from a country or territory other than Bermuda where they are subject to equivalent requirements (and are supervised for compliance with those requirements), and which hold client money in pooled accounts, are obliged to verify the identities of their clients. Institutions with which such client accounts are held are not required to identify the beneficial owners of such funds, provided that the information on the identity of the beneficial owner is available, on request, to the institution.

Partnerships and unincorporated businesses

- 5.187 Partnerships and unincorporated businesses, although principally operated by individuals, or groups of individuals, are different from private individuals in that there is an underlying business. This business is likely to have a different money laundering or terrorist financing risk profile from that of an individual.

Regulation 3(2)

- 5.188 The beneficial owner of a partnership is any individual who ultimately is entitled to or controls (whether the entitlement or control is direct or indirect) more than a 25% share of the capital or profits of the partnership, or more than 25% of the voting rights in the partnership, or who otherwise exercises control over the management of the partnership.

Obtain standard evidence

- 5.189 The institution should obtain the following in relation to the partnership or unincorporated association:

- Full name;
- Business address;
- Names of all partners/principals who exercise control over the management of the partnership; and
- Names of individuals who own or control over 25% of its capital or profit, or of its voting rights.

- 5.190 Given the wide range of partnerships and unincorporated businesses, in terms of size, reputation and numbers of partners/principals, institutions need to make an assessment of where a particular partnership or business lies on the associated risk spectrum.

- 5.191 The institution's obligation is to verify the identity of the customer using evidence from a reliable and independent source. Where partnerships or unincorporated businesses are well-known, reputable organisations, with long histories in their industries and with substantial public information about them and their principals and controllers, confirmation of the customer's membership of a relevant professional or trade association is likely to be able to provide such reliable and independent evidence. This does not obviate the need to verify the identity of the partnership's beneficial owners.

- 5.192 Other partnerships and unincorporated businesses will have a lower profile and will generally comprise a much smaller number of partners/principals. In verifying the identity of such customers, institutions should primarily have regard to the number of partner/principals. Where these are relatively few, the customer should be treated as a collection of private individuals, and the institution should follow the guidance set out in paragraphs 5.67 to 5.103; where numbers are larger the institution should decide whether it should continue to regard the customer as a collection of private individuals, or whether it can be satisfied with evidence of membership of a relevant professional or trade association. In either circumstance, there is likely to be a need to see the partnership deed to be satisfied that the entity exists, unless an entry in an appropriate register may be checked.

5.193 Institutions should take appropriate steps to be reasonably satisfied that the person the institution is dealing with is properly authorised by the customer.

5.194 Some consideration should be given as to whether documents relied upon are forged. In addition, if they are in a foreign language, appropriate steps should be taken to be reasonably satisfied that the documents in fact provide evidence of the customer's identity.

Variation from the standard

5.195 Most partnerships and unincorporated businesses are smaller less transparent and less well known entities, and are not subject to the same accountability requirements as, for example, companies listed on the Bermuda Stock Exchange.

5.196 Where the money laundering or terrorist financing risk is considered to be at its lowest, the institution may be able to use the source of funds as evidence of the customer's identity. The guidance in paragraphs 5.92 to 5.96 should be followed. This does not obviate the need to verify the identity of beneficial owners, where these exist.

5.197 Whenever faced with less transparency, less of an industry profile, or less independent means of verification of the client entity, institutions should consider the money laundering or terrorist financing risk presented by the entity, and therefore the extent to which, in addition to the standard evidence, additional precautions should be taken.

5.198 It is important to know and understand any associations the entity may have with other jurisdictions (headquarters, operating facilities, branches, subsidiaries, etc) and the individuals who may influence its operations (political connections, etc).

Principals and owners

5.199 Following its assessment of the money laundering or terrorist financing risk presented by the entity, the institution may decide to verify the identity of one or more of the partners/owners as customers. In that event, verification requirements are likely to be appropriate for partners/owners who have authority to operate an account or to give the institution instructions concerning the use or transfer of funds or assets; other partners/owners must be verified as beneficial owners, following the guidance in paragraphs 5.33 & 5.34.

Clubs and societies

5.200 Where an application is made on behalf of a club or society, institutions should make appropriate distinction between those that serve a limited social or local purpose and those where the activities and connections are more sophisticated or are geographically based and/or with financial links to other countries.

5.201 For the vast majority of clubs and societies, either there will be no individual who is a beneficial owner within the meaning of the Regulations or at most a class of persons who stand to benefit from the club or society's objects that must be identified. These persons will be self-evident from a review of the club or society's objects in its constitution.

Obtain standard evidence

5.202 For many clubs and societies, the money laundering or terrorist financing risk will be low. The following information should be obtained about the customer:

- Full name of the club/society;
- Legal status of the club/society;
- Purpose of the club/society; and
- Names of all officers.

- 5.203 The institution should verify the identities of the officers who have authority to operate an account or to give the institution instructions concerning the use or transfer of funds or assets.
- 5.204 Institutions should take appropriate steps to be reasonably satisfied that the person they are dealing with is properly authorised by the customer.
- 5.205 Some consideration should be given as to whether documents relied upon are forged. In addition, if they are in a foreign language, appropriate steps should be taken to be reasonably satisfied that the documents in fact provide evidence of the customer's identity.

Variation from the standard

- 5.206 Where the money laundering or terrorist financing risk is considered to be at its lowest, the institution may be able to use the source of funds as evidence of the customer's identity. The guidance in paragraphs 5.92 to 5.96 should be followed. This does not obviate the need to verify the identity of beneficial owners, where these exist.
- 5.207 The institution's risk assessment may lead it to conclude that the money laundering or terrorist financing risk is higher and that it should require additional information on the purpose, funding and beneficiaries of the club or society.
- 5.208 Following its assessment of the money laundering or terrorist financing risk presented by the club/society, the institution may decide to verify the identities of additional officers, and/or institute additional transaction monitoring arrangements (see paragraphs 5.283 to 5.303).

Simplified due diligence

Regulation 10(1) & 6(3)(b)

- 5.209 Simplified due diligence means not having to apply customer due diligence measures. In practice, this means not having to identify the customer or to verify the customer's identity or, where relevant, that of a beneficial owner, nor having to obtain information on the purpose or intended nature of the business relationship. It is, however, still necessary to conduct on-going monitoring of the business relationship. Institutions must have reasonable grounds for believing that the customer, transaction or product relating to such transaction falls within one of the categories set out in the Regulations and may have to demonstrate this to the BMA. Clearly, for operating purposes, the institution will still need to maintain a base of information about the customer.

Regulation 10

- 5.210 Simplified due diligence may be applied when the customer is:
- An institution subject to the Regulations;
 - An institution (or equivalent institution) which is situated in a country or territory other than Bermuda which imposes requirements equivalent to the Regulations and is supervised for compliance with those requirements;
 - Companies listed on an appointed stock exchange;
 - an independent professional where the product is an account into which monies are pooled and information on the identity of the person on whose behalf monies are held is available on request to the institution acting as custodian for the account;
 - A public authority in Bermuda;
 - Certain life insurance products;
 - Certain pension funds; or
 - Certain low-risk products.

Regulation 6(1) (c) & (d)

- 5.211 There is no exemption from the obligation to verify identity where the institution suspects that a proposed relationship or occasional transaction may involve money laundering or terrorist financing, or where there are doubts about the veracity or accuracy of documents, data or information previously obtained for the purposes of customer verification.

Regulation 10(6) (c)

- 5.212 Simplified due diligence may be applied to pension, superannuation or similar schemes which provide retirement benefits to employees, where contributions are made by an employer or by way of deduction from an employee's wages and the scheme rules do not permit the assignment of a member's interest under the scheme.

Regulation 10(7) and the Schedule, paragraph 1

- 5.213 Simplified due diligence may be applied to low-risk products which meet specified criteria set out in the Regulations. These criteria, which are cumulative, are:

- The product has a written contractual base;
- Any related transactions are carried out through an account of the customer with a bank which is subject to these Regulations, or a bank situated in a country or territory other than Bermuda which imposes requirements equivalent to those laid down in these Regulations;
- The product or related transaction is not anonymous and its nature is such that it allows for the timely application of customer due diligence measures where there is a suspicion of money laundering or terrorist financing;
- The product is within the following maximum threshold:
 - a) in the case of insurance policies or savings products of a similar nature, the annual premium is no more than \$1,000 or there is a single premium of no more than \$2,500;
 - b) in the case of products which are related to the financing of physical assets where the legal and beneficial title of the assets is not transferred to the customer until the termination of the contractual relationship (whether the transaction is carried out in a single operation or in several operations which appear to be linked) the annual payments do not exceed \$15,000;
 - c) in all other cases, the maximum threshold is \$15,000.
- The benefits of the product or related transaction cannot be realised for the benefit of third parties, except in the case of death, disablement, survival to a predetermined advanced age, or similar events;
- In the case of products or related transactions allowing for the investment of funds in financial assets or claims, including insurance or other kinds of contingent claims:
 - a) the benefits of the product or related transaction are only realisable in the long term;
 - b) the product or related transaction cannot be used as collateral;
 - c) during the contractual relationship, no accelerated payments are made, surrender clauses used or early termination takes place.

Regulation 10(7)

- 5.214 Institutions need to decide whether particular products meet the criteria for simplified due diligence.

Regulations (5) and (7)

- 5.215 An exemption from the basic verification obligation does not extend to the obligation to conduct on-going monitoring of the business relationship, or to the duty to report knowledge or suspicion of money laundering or terrorist financing.

Enhanced due diligence

Regulation 11(1)

- 5.216 An institution must apply enhanced customer due diligence measures on a risk-sensitive basis in any situation which by its nature can present a higher-risk of money laundering or terrorist financing. As part of this, an institution may conclude, under its risk based approach, that the standard evidence of identity (see paragraphs 5.24 to 5.208) is insufficient in relation to the money laundering or terrorist financing risk, and that it must obtain additional information about a particular customer.
- 5.217 As a part of a risk-based approach therefore, institutions may need to hold sufficient information about the circumstances and business of their customers for two principal reasons:
- To inform its risk assessment process and thus manage its money laundering/terrorist financing risks effectively; and
 - To provide a basis for monitoring customer activity and transactions, thus increasing the likelihood that they will detect the use of their products and services for money laundering and terrorist financing.
- 5.218 The extent of additional information sought and of any monitoring carried out in respect of any particular customer, or class/category of customer, will depend on the money laundering or terrorist financing risk that the customer, or class/category of customer, is assessed to present to the institution.
- 5.219 In practice, under a risk-based approach, it will not be appropriate for every product or service provider to know their customers equally well, regardless of the purpose, use, value, etc., of the product or service provided. Institutions' information demands need to be proportionate, appropriate and discriminating and to be able to be justified to customers.
- 5.220 An institution should hold a fuller set of information in respect of those customers or class/category of customers, assessed as carrying a higher money laundering or terrorist financing risk, or who are seeking a product or service that carries a higher-risk of being used for money laundering or terrorist financing purposes.
- 5.221 When someone becomes a new customer or applies for a new product or service, the institution may, depending on the nature of the product or service for which they are applying, request information as to the customer's residential status, employment details, income, and other sources of income, in order to decide whether to accept the application.
- 5.222 The availability and use of other financial information held is important for reducing the additional costs of collecting customer information. Where appropriate and practical, therefore, institutions should take reasonable steps to ensure that, where they have customer information in one part of the business, they are able to link it to information in another.

Regulation 11

- 5.223 The Regulations prescribe three specific types of relationship in respect of which enhanced due diligence measures must be applied. These are:
- Where the customer has not been physically present for identification purposes;
 - In respect of a correspondent banking relationship; and
 - In respect of a business relationship or occasional transaction with a PEP.

Non face-to-face identification and verification

- 5.224 Whilst some types of financial transactions have traditionally been conducted on a non-face-to-face basis, other types of transactions and relationships are increasingly being undertaken in this way: e.g., internet and telephone banking and online share dealing.

5.225 Although applications and transactions undertaken across the internet may in themselves not pose any greater risk than other non face-to-face business, such as applications submitted by post, there are other factors that may, taken together, aggravate the typical risks:

- The ease of access to the facility, regardless of time and location;
- The ease of making multiple fictitious applications without incurring extra cost or the risk of detection;
- The absence of physical documents; and
- The speed of electronic transactions.

Regulation 11(2)

5.226 Where the customer has not been physically present for identification purposes, an institution must take specific and adequate measures to compensate for the higher-risk, for example by applying one or more of the following measures:

- Ensuring that the customer's identity is established by additional documents, data or information;
- Supplementary measures to verify or certify the documents supplied, or requiring confirmatory certification by an institution in an equivalent jurisdiction; or
- Ensuring that the first payment of the operation is carried out through an account opened in the customer's name with a bank.

5.227 The extent of verification in respect of non face-to-face customers will depend on the nature and characteristics of the product or service requested and the assessed money laundering or terrorist financing risk presented by the customer. There are some circumstances where the customer is typically not physically present - such as in many wholesale markets, or when purchasing some types of collective investments - which would not in themselves increase the risk attaching to the transaction or activity. An institution should take account of such cases in developing their systems and procedures.

5.228 Additional measures would also include assessing the possibility that the customer is deliberately avoiding face-to-face contact. It is therefore important to be clear on the appropriate approach in these circumstances.

5.229 Where a customer approaches an institution remotely (by post, telephone or over the internet), the institution should carry out non face-to-face verification, either electronically (see paragraphs 5.79 to 5.82), or by reference to documents (see paragraphs 5.69 to 5.78).

5.230 Non face-to-face identification and verification carries an inherent risk of impersonation fraud and institutions should follow the guidance in paragraph 5.83 to mitigate this risk.

Politically Exposed Persons (PEPs)

5.231 Individuals who have or have had a high political profile, or hold or have held public office, can pose a higher money laundering or terrorist financing risk to institutions as their position may make them vulnerable to corruption. This risk also extends to members of their immediate families and to known close associates. PEP status itself does not, of course, incriminate individuals or entities. It does, however, put the customer or the beneficial owner, into a higher-risk category.

Regulation 11(4),(5),(6) & (7)

5.232 A PEP is defined as "an individual who is or has, in a country or territory outside Bermuda, at any time in the preceding year, been entrusted with prominent public functions and an immediate family member, or a known close associate, of such a person".

5.233 Although under the definition of a PEP an individual ceases to be so regarded after he has left office for one year, institutions are encouraged to apply a risk-based approach in determining whether they should cease carrying out appropriately enhanced monitoring of his transactions or activity at the end of this

period. In many cases, a longer period might be appropriate, in order to ensure that the higher-risks associated with the individual's previous position have adequately abated.

Regulations - Schedule, paragraph 2(1)(a)

5.234 Public functions exercised at levels lower than national should normally not be considered prominent. However, when their political exposure is comparable to that of similar positions at national level, institutions should consider, on a risk-based approach, whether persons exercising those public functions should be considered as PEPs. Prominent public functions include:

- Heads of state, heads of government, ministers and deputy or assistant ministers;
- Members of parliaments;
- Members of supreme courts, of constitutional courts or of other high level judicial bodies whose decisions are not generally subject to further appeal, except in exceptional circumstances;
- Members of the boards of central banks;
- Ambassadors, charges d'affaires and high-ranking officers in the armed forces; and
- Members of the administration, management or supervisory bodies of State-owned enterprises.

These categories do not include middle-ranking or more junior officials.

Regulations - Schedule, paragraph 2(1)(d)

5.235 Immediate family members include:

- A spouse;
- A partner (including a person who is considered by national law as equivalent to a spouse);
- Children and their spouses or partners; and
- Parents.

Regulations - Schedule, paragraph 2 (1)(e)

5.236 Persons known to be close associates include:

- Any individual who is known to have joint beneficial ownership of a legal entity or legal arrangement, or any other close business relations, with a person who is a PEP; and
- Any individual who has sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the benefit of a person who is a PEP.

Regulation 11(7) and 16(2)(c)

5.237 For the purpose of deciding whether a person is a known close associate of a PEP, the institution need only have regard to any information which is in its possession, or which is publicly known. Having to obtain knowledge of such a relationship does not presuppose active research by the institution.

Regulation 11(4)

5.238 Institutions are required, on a risk-sensitive basis, to:

- Have appropriate risk-based procedures to determine whether a customer is a PEP;
- Obtain appropriate senior management approval for establishing a business relationship with such a customer;
- Take adequate measures to establish the source of wealth and source of funds which are involved in the business relationship or occasional transaction; and
- Conduct on-going monitoring of the business relationship.

Risk-based procedures

5.239 The nature and scope of a particular institution's business will generally determine whether the existence of PEPs in their customer base is an issue for the institution, and whether or not the institution needs to screen all customers for this purpose. In the context of this risk analysis, it would be appropriate if the institution's resources were focused in particular on products and transactions that are characterised by a high-risk of money laundering or terrorist financing.

5.240 Establishing whether individuals qualify as PEPs is not always straightforward and can present difficulties. Where institutions need to carry out specific checks, they may be able to rely on an internet search engine, or consult relevant reports and databases on corruption risk published by specialised national, international, non-governmental and commercial organisations. Resources such as the Transparency International Corruption Perceptions Index, [2008/cpi/surveys indices/policy research](#) which ranks approximately 150 countries according to their perceived level of corruption, may be helpful in terms of assessing the risk. If there is a need to conduct more thorough checks, or if there is a high likelihood of an institution having PEPs for customers, subscription to a specialist PEP database may be the only adequate risk mitigation tool.

Senior management approval

5.241 Obtaining approval from senior management for establishing a business relationship does not mean obtaining approval from the Board of directors (or equivalent body), but from the immediately higher level of authority to the person seeking such approval.

On-going monitoring

5.242 Guidance on the on-going monitoring of the business relationship is given in paragraphs 5.283 to 5.303. Institutions should remember that new and existing customers may not initially meet the definition of a PEP, but may subsequently become one during the course of a business relationship. The institution should, as far as practicable, be alert to public information relating to possible changes in the status of its customers with regard to political exposure. When an existing customer is identified as a PEP, enhanced customer due diligence must be applied to that customer.

5.243 Frequently, a customer may have contact with two or more institutions in respect of the same transaction. This can be the case in both the retail market, where customers are routinely introduced by one institution to another, or deal with one institution through another, and in some wholesale markets, such as syndicated lending, where several institutions may participate in a single loan to a customer. However, several institutions requesting the same information from the same customer in respect of the same transaction not only does not help in the fight against financial crime, but also adds to the inconvenience to the customer. It is important, therefore, that in all circumstances each institution is clear as to its relationship with the customer and its related AML/ATF obligations, and as to the extent to which it can rely upon or otherwise take account of the verification of the customer that another institution has carried out. Such account must be taken in a balanced way that appropriately reflects the money laundering or terrorist financing risks. Account must also be taken of the fact that some of the institutions involved may not be Bermuda based.

5.244 In other cases, a customer may be an existing customer of another institution in the same group. Guidance on meeting AML/ATF obligations in such a relationship is given in paragraphs 5.265 to 5.268.

Multipartite relationships, including reliance on third parties

Reliance on third parties

Regulation 14

5.245 The Regulations expressly permit an institution to rely on another person to apply any or all of the customer due diligence measures, provided that the other person is listed in Regulation 14(2), and that consent to being relied on has been given (see paragraph 5.248). The relying institution, however, retains responsibility for any failure to comply with a requirement of the Regulations, as this responsibility cannot be delegated.

5.246 For example:

- Where an institution (institution A) enters into a business relationship with, or undertakes an occasional transaction for, the underlying customer of another institution (institution B), for example by accepting instructions from the customer (given through Institution B); or
- Institution A and institution B both act for the same customer in respect of a transaction (e.g., institution A as executing broker and institution B as clearing broker), institution A may rely on institution B to carry out customer due diligence measures, while remaining ultimately liable for compliance with the Regulations.

Regulation 14(2) (a) & (b)

5.247 In this context, Institution B must be:

- (1) a person who carries on business in Bermuda who is an AML/ATF regulated financial institution under section 2(2) of the Regulations or a business in the regulated sector under section 3 of the Anti-Terrorism (Financial and Other Measures) (Business in Regulated Sector) Order 2008; or
- (b) an independent professional as defined at section (2)(1) of the Regulations.

Regulation 14(2)(c)

- (2) a person who carries on business in a country or territory other than Bermuda who is:
 - (a) an institution that carries on business corresponding to the business of an AML/ATF regulated financial institutions or independent professionals;
 - (b) subject to mandatory professional registration recognised by law;
 - (c) subject to requirements equivalent to those laid down in the regulations; and
 - (d) supervised for compliance with those requirements in a manner equivalent to supervision by the relevant supervisory authority.

Consent to be relied upon

5.248 The Regulations do not define how consent must be evidenced. Ordinarily, 'consent' means an acceptance of some form of proposal by one party from another – this may be written or oral, express or implied. Written acknowledgement that an institution is being relied on makes its relationship with the institution relying on it clear. On the other hand, it is not necessary for an institution to give an express indication that it is being relied on, and it may be inferred from their conduct; for example - dealing with an institution after receipt of that institution's terms of business which indicate reliance; silence where it has been indicated that this would be taken as acknowledgement of reliance; participation in a tri-partite arrangement, based on a market practice that has reliance as an integral part of its framework.

5.249 In order to satisfy the purpose behind Regulation 14(1)(a), an institution may wish to consider providing the institution being relied on with notification of the reliance. The notification should specify that the institution intends to rely on the third party institution for the purposes of Regulation 14(1)(a). Such a notification can be delivered in a number of ways. For example, where one institution is introducing a client to another institution, the issue of reliance can be raised during the introduction process and may form part of the formal agreement with the intermediary. Similarly, where the relying and relied upon institutions are party to tripartite agreement with a client, the notification may be communicated during exchange of documents. Where a relationship exists between the parties it is likely that such a notification plus some form of acceptance (see paragraph 5.248) should be sufficient for the purposes of establishing consent.

5.250 Where there is no contractual or commercial relationship between the relying and relied on institutions it is less likely that consent can be assumed from the silence of the institution being relied on. In such circumstances institutions may wish to seek an express agreement as to reliance. This does not need to take the form of a legal agreement and a simple indication of consent (e.g., by e-mail) should suffice.

Basis of reliance

- 5.251 For one institution to rely on verification carried out by another institution, the verification that the institution being relied upon has carried out must have been based at least on the standard level of customer verification. It is not permissible to rely on simplified due diligence carried out, or any other exceptional form of verification, such as the use of source of funds as evidence of identity.
- 5.252 Institutions may also only rely on verification actually carried out by the institution being relied upon. An institution that has been relied on to verify a customer's identity may not 'pass on' verification carried out for it by another institution.
- 5.253 Whether an institution wishes to place reliance on a third party will be part of the Institution's risk-based assessment, which, in addition to confirming the third party's status (Regulation 14(2)), may include consideration of matters such as:
- Its public disciplinary record, to the extent that this is available;
 - The nature of the customer, the product/service sought and the sums involved;
 - Any adverse experience of the other institution's general efficiency in business dealings; and
 - Any other knowledge, whether obtained at the outset of the relationship or subsequently, that the institution has regarding the standing of the institution to be relied upon.
- 5.254 The assessment as to whether or not an institution should accept confirmation from a third party that appropriate customer due diligence measures have been carried out on a customer will be risk-based, and cannot be based simply on a single factor.
- 5.255 In practice, the institution relying on the confirmation of a third party needs to know:
- The identity of the customer and/or beneficial owner whose identity is being verified;
 - The level of customer due diligence that has been carried out; and
 - Confirmation of the third party's understanding of his obligation to make available, on request, copies of the verification data, documents or other information. In order to standardise the process of institutions confirming to one another that appropriate customer due diligence measures have been carried out on customers, guidance is given in paragraphs 5.269 to 5.272 below on the use of pro-forma confirmations containing the above information.
- 5.256 The third party has no obligation to provide such confirmation to the product/service provider, and may choose not to do so. In such circumstances, or if the product/service provider decides that it does not wish to rely upon the third party, then the institution must carry out its own customer due diligence measures on the customer.
- 5.257 For an institution to confirm that it has carried out customer due diligence measures in respect of a customer is a serious matter. An institution must not give a confirmation on the basis of a generalised assumption that the institution's systems have operated effectively. There has to be awareness that the appropriate steps have in fact been taken in respect of the customer that is the subject of the confirmation.

Regulation 15(5)

- 5.258 An institution which carries on business in Bermuda and is relied on by another person must, within the period of five years beginning on the date on which it is relied on, if requested by the institution relying on it:
- As soon as reasonably practicable make available to the institution which is relying on it any information about the customer (and any beneficial owner) which the third party obtained when applying customer due diligence measures; and
 - As soon as reasonably practicable forward to the institution which is relying on it relevant copies of any identification and verification data and other relevant documents on the identity of the customer (and any beneficial owner) which the third party obtained when applying those measures.

Regulation 15(6)

- 5.259 An institution which relies on an institution situated in a country or territory other than Bermuda to apply customer due diligence measures must take steps to ensure that the institution on which it relies will, within the period of five years beginning on the date on which the third party is relied on, if requested, comply with the obligations set out in paragraph 5.258.
- 5.260 The personal information supplied by the customer as part of a third party's customer identification procedures will generally be set out in the form that the relying institution will require to be completed, and this information will therefore be provided to that institution.

Regulation 15(5) & (6)

- 5.261 A request to forward copies of any identification and verification data and other relevant documents on the identity of the customer or beneficial owner obtained when applying customer due diligence measures, if made, would normally be as part of an institution's risk-based customer acceptance procedures. However, the institution giving the confirmation must be prepared to provide this data or other relevant documents throughout the five year period for which it has an obligation under the Regulations to retain them.
- 5.262 Where an institution makes such a request and it is not met, the institution will need to take account of that fact in its assessment of the third party in question, and of the ability to rely on the third party in the future. In addition, the institution should review its application of CDD in respect of the customer or beneficial owner in question.
- 5.263 An institution must also document the steps taken to confirm that the institution relied upon satisfies the requirements in Regulation 14(2). This is particularly important where the institution relied upon is situated in a country or territory other than Bermuda.
- 5.264 Part of the institution's AML/ATF policy statement should address the circumstances where reliance may be placed on other institutions and how the institution will assess whether the other institution satisfies the definition of third party in Regulation 14(2) (see paragraph 5.247).

Group introductions

- 5.265 Where customers are introduced between different parts of the same financial sector group, entities that are part of the group should be able to rely on identification procedures conducted by that part of the group which first dealt with the customer. One member of a group should be able to confirm to another part of the group that the identity of the customer has been appropriately verified.
- 5.266 Where a customer is introduced by one part of a financial sector group to another, it is not necessary for his identity to be re-verified, provided that:
- The identity of the customer has been verified by the introducing part of the group in line with AML/ATF standards of Bermuda or an equivalent jurisdiction; and
 - The group entity that carried out the customer due diligence measures can be relied upon as a third party under Regulation 14(2).
- 5.267 The acceptance by a Bermuda institution of confirmation from another group entity that the identity of a customer has been satisfactorily verified is dependent on the relevant records being readily accessible, on request, from the other entity.
- 5.268 Where Bermuda institutions have day-to-day access to all group customer information and records, there is no need to obtain a group introduction confirmation, if the identity of that customer has been verified previously to AML/ATF standards in Bermuda, or in an equivalent jurisdiction. However, if the identity of the customer has not previously been verified, for example because the group customer relationship pre-

dates the introduction of AML/ATF regulations, or if the verification evidence is inadequate, any missing verification evidence will need to be obtained.

Use of pro-forma confirmations

Regulation 14(2)

- 5.269 Whilst an institution may be able to place reliance on another party to apply all or part of the customer due diligence measures under Regulation 14(2) (see paragraph 5.245), it may still wish to receive, as part of its risk-based procedures, a written confirmation from the third party, not least to evidence consent. This may also be the case, for example, when an institution is unlikely to have an on-going relationship with the third party. Confirmations can be particularly helpful when dealing with third parties located in a country or territory other than Bermuda, where it is necessary to confirm that the relevant records will be available (see 5.258).
- 5.270 The provision of a confirmation certificate implies consent to be relied upon, in accordance with paragraph 5.248.
- 5.271 Pro-forma confirmations for customer identification and verification are attached as Annex 5-I to 5-IV to this chapter.
- 5.272 Pro-forma confirmations in respect of group introductions are attached as Annex 5-V to 5-VI to this chapter.

Situations which are not reliance

One institution acting solely as introducer

- 5.273 At one end of the spectrum, one institution may act solely as an introducer between the customer and the institution providing the product or service, and may have no further relationship with the customer. The introducer plays no part in the transaction between the customer and the institution, and has no relationship with either of these parties that would constitute a business relationship.
- 5.274 In these circumstances, where the introducer neither gives advice nor plays any part in the negotiation or execution of the transaction, the identification and verification obligations under the Regulations lie with the product/service provider. This does not, of course, preclude the introducing entity carrying out identification and verification of the customer on behalf of the institution providing the product or service, as agent for that institution (see paragraphs 5.275 & 5.276).

Where the intermediary is the agent of the product/service provider

- 5.275 If the intermediary is an agent or appointed representative of the product or service provider, it is an extension of that institution. The intermediary may actually obtain the appropriate verification evidence in respect of the customer, but the product/service provider is responsible for specifying what should be obtained, and for ensuring that records of the appropriate verification evidence taken in respect of the customer are retained.
- 5.276 Similarly, where the product/service provider has a direct sales force, they are part of the institution, whether or not they operate under a separate group legal entity. The institution is responsible for specifying what is required, and for ensuring that records of the appropriate verification evidence taken in respect of the customer are retained.

Where the intermediary is the agent of the customer

- 5.277 From the point of view of a product/service provider, the position of an intermediary, as agent of the customer, is influenced by a number of factors. The intermediary may be subject to the Regulations or to similar legislation in an equivalent jurisdiction.

Regulation 10(2)

- 5.278 Depending on jurisdiction, where the customer is an intermediary carrying on appropriately regulated business, and is acting on behalf of another, there is no obligation on the product provider to carry out customer due diligence measures on the customer, or on the underlying party.
- 5.279 Where an institution cannot apply simplified due diligence to the intermediary (see paragraphs 5.209 to 5.215), the product/service provider is obliged to carry out customer due diligence measures on the intermediary and, as the intermediary acts for another, on the underlying customer.
- 5.280 Where the institution takes instruction from the underlying customer, or where the institution acts on the underlying customer's behalf (e.g., as a custodian) the institution then has an obligation to carry out customer due diligence measures in respect of that customer, although the reliance provisions (see paragraphs commencing at 5.245) may be applied.
- 5.281 In these circumstances, in verifying the identity of the underlying customer, the institution should take a risk-based approach. It will need to assess the AML/ATF regime in the intermediary's jurisdiction, the level of reliance that can be placed on the intermediary and the verification work it has carried out, and as a consequence, the amount of evidence that should be obtained direct from the customer.
- 5.282 In particular, where the intermediary is located in a higher-risk jurisdiction, the risk-based approach should be aimed at ensuring that the business does not proceed unless the identity of the underlying customer has been verified to the product/service provider's satisfaction.

Monitoring customer activity

The requirement to monitor customers' activities

Regulation 7

- 5.283 Institutions must conduct on-going monitoring of the business relationship with their customers. On-going monitoring of a business relationship includes:
- Scrutiny of transactions undertaken throughout the course of the relationship (including, where necessary, the source of funds) to ensure that the transactions are consistent with the institution's knowledge of the customer, his business and risk profile; and
 - Ensuring, as far as practicable, that the documents, data or information held by the institution are kept up to date.
- 5.284 Monitoring customer activity helps identify unusual activity. If unusual activities cannot be rationally explained, they may involve money laundering or terrorist financing. Monitoring customer activity and transactions that take place throughout a relationship helps institutions know their customers, assist them to assess risk and provides greater assurance that the institution is not being used for the purposes of financial crime.

What is monitoring?

- 5.285 The essentials of any system of monitoring are that:
- It flags up transactions and/or activities for further examination;
 - These reports are reviewed promptly by the right person(s); and
 - Appropriate action is taken on the findings of any further examination.

5.286 Monitoring can be either:

- In real time, in that transactions and/or activities can be reviewed as they take place or are about to take place; or
- After the event, through some independent review of the transactions and/or activities that a customer has undertaken.

and in either case unusual transactions or activities will be flagged for further examination.

5.287 Monitoring may be by reference to specific types of transactions, to the profile of the customer, or by comparing their activity or profile with that of a similar peer group of customers, or through a combination of these approaches.

5.288 Institutions should also have systems and procedures to deal with customers who have not had contact with the institution for some time, in circumstances where regular contact might be expected, and with dormant accounts or relationships, to be able to identify future reactivation and unauthorised use.

5.289 In designing monitoring arrangements, it is important that appropriate account be taken of the frequency, volume and size of transactions with customers, in the context of the assessed customer and product risk.

5.290 Monitoring is not a mechanical process and does not necessarily require sophisticated electronic systems. The scope and complexity of the process will be influenced by the institution's business activities, and whether the institution is large or small. The key elements of any system are having up-to-date customer information, on the basis of which it will be possible to spot the unusual, and asking pertinent questions to elicit the reasons for unusual transactions or activities in order to judge whether they may represent something suspicious.

Nature of monitoring

5.291 Some financial services business typically involves transactions with customers about whom the institution has a good deal of information, acquired for both business and regulatory reasons. Other types of financial services business involve transactions with customers about whom the institution may need to have only limited information. The nature of the monitoring in any given case will therefore depend on the business of the institution, the frequency of customer activity, and the types of customer that are involved.

5.292 Effective monitoring is likely to be based on a considered identification of transaction characteristics, such as:

- The unusual nature of a transaction: e.g., abnormal size or frequency for that customer or peer group; the early surrender of an insurance policy;
- The nature of a series of transactions: for example, a number of cash credits;
- The geographic destination or origin of a payment: for example, to or from a high-risk country; and
- The parties concerned: for example, a request to make a payment to or from a person on a sanctions list.

5.293 The arrangements should include the training of staff on procedures to spot and deal specially (e.g., by referral to management) with situations that arise that suggest a heightened money laundering or terrorist financing risk; or they could involve arrangements for exception reporting by reference to objective triggers (e.g., transaction amount). Staff training is not, however, a substitute for having in place some form of regular monitoring activity.

Regulation 11(1)

5.294 Higher risk accounts and customer relationships require enhanced customer due diligence and on-going monitoring. This will generally mean more frequent or intensive monitoring.

Manual or automated?

- 5.295 A monitoring system may be manual, or may be automated to the extent that a standard suite of exception reports are produced. One or other of these approaches may suit most institutions. In the relatively few institutions where there are major issues of volume, or where there are other factors that make a basic exception report regime inappropriate, a more sophisticated automated system may be necessary.
- 5.296 It is essential to recognise the importance of staff alertness. Such factors as staff intuition, direct exposure to a customer face-to-face or on the telephone, and the ability, through practical experience, to recognise transactions that do not seem to make sense for that customer, cannot be automated (see Chapter 7: Staff awareness, training and alertness).
- 5.297 In relation to an institution's monitoring needs, an automated system may add value to manual systems and controls, provided that the parameters determining the outputs of the system are appropriate. Institutions should understand the workings and rationale of an automated system, and should understand the reasons for its output of alerts, as it may be asked to explain this to its regulator.
- 5.298 The greater the volume of transactions, the less easy it will be for an institution to monitor them without the aid of some automation. Systems available include those that many institutions, particularly those that offer credit, use to monitor fraud. Although not specifically designed to identify money laundering or terrorist financing, the output from these anti-fraud monitoring systems can often indicate possible money laundering or terrorist financing.
- 5.299 There are many automated transaction monitoring systems available on the market and they use a variety of techniques to detect and report unusual/uncharacteristic activity. These techniques can range from artificial intelligence to simple rules. The systems available are not designed to detect money laundering or terrorist financing but are able to detect and report unusual/uncharacteristic behaviour by customers, and patterns of behaviour that are characteristic of money laundering or terrorist financing, which after analysis may lead to suspicion of money laundering or terrorist financing. The implementation of transaction monitoring systems is difficult due to the complexity of the underlying analytics used and their heavy reliance on customer reference data and transaction data.
- 5.300 Monitoring systems, manual or automated, can vary considerably in their approach to detecting and reporting unusual or uncharacteristic behaviour. It is important for institutions to ask questions of the supplier of an automated system, and internally within the business, whether in support of a manual or an automated system, to aid them in selecting a solution that meets their particular business needs best. Questions that should be addressed include:
- How does the solution enable the institution to implement a risk-based approach to customers, third parties and transactions?
 - How do system parameters aid the risk-based approach and consequently affect the quality and volume of transaction alerts?
 - What are the money laundering/terrorist financing typologies that the system addresses, and which component of the system addresses each typology? Are the typologies that are included with the system complete? Are they relevant to the institution's particular line of business?
 - What functionality does the system provide to implement new typologies, how quickly can relevant new typologies be commissioned in the system and how can their validity be tested prior to activation in the live system?
 - What functionality exists to provide the user with the reason that a transaction is flagged and is there full evidential process behind the reason given?
 - Does the system have robust mechanisms to learn from previous experience and how is the false positive rate continually monitored and reduced?
- 5.301 What constitutes unusual or uncharacteristic behaviour by a customer is often defined by the system. It will be important that the system selected has an appropriate definition of 'unusual or uncharacteristic' and one that is in line with the nature of business conducted by the institution.

- 5.302 The effectiveness of a monitoring system, automated or manual, in identifying unusual activity will depend on the quality of the parameters which determine what alerts it makes, and the ability of staff to assess and act as appropriate on these outputs. The needs of each institution will therefore be different, and each system will vary in its capabilities according to the scale, nature and complexity of the business. It is important that the balance is right in setting the level at which an alert is generated; it is not enough to fix it so that the system generates just enough output for the existing staff complement to deal with – but equally, the system should not generate large numbers of ‘false positives’, which require excessive resources to investigate.
- 5.303 Monitoring also involves keeping information held about customers up to date, as far as practicable. Guidance on this is given at paragraph 5.45.

Persons institutions should not accept as customers

- 5.304 The United Nations has adopted sanctions to deny a range of named individuals and organisations, as well as nationals from certain countries, access to the financial services sector (*Guidance Notes - page 10 paragraph 1.8*) and some of the relevant United Nations sanctions include SCR 1267 (1999), 1373 (2001), 1390 (2002) and 1617 (2005).
- 5.305 On the 28th September 2001 the United Nations Security Council adopted resolution 1373. The United Kingdom government passed **The Terrorism (United Nations Measures) (Overseas Territories) Order 2001** giving effect to resolution 1373. The Order applies to Bermuda and prohibits fund raising for terrorism purposes, restricts the making available of funds and financial services to terrorist organisations and provides powers to freeze accounts of suspected terrorist organisations. Under section 8 of the Order, relevant institutions (which are defined, but include deposit taking institutions) commit an offence if they fail to report to the Governor if they become aware, or suspect that a customer has been involved in the commission of offences under the Order or is controlled or owned by a person who has committed such offences.
- 5.306 On the 16th January 2002 the United Nations Security Council adopted resolution 1390. The United Kingdom government passed **The Al-Qa’ida and Taliban (United Nations Measures) (Overseas Territories) Order 2002** giving effect to resolution 1390. This Order applies to Bermuda and prohibits the making of funds available, the delivery or supply of arms and related material, technical assistance or training to listed persons. That term is defined as including Usama bin Laden, any person designated by the Sanctions Committee in the list maintained in accordance with Resolution 1390 as members of Al-Qa’ida, members of the Taliban or groups, undertakings or entities associated with any of the above. The Order also contains powers for the Governor to issue a Notice freezing funds if there are reasonable grounds for suspecting that the holder may be a listed person or holding funds on behalf of a listed person. Section 10 of the Order makes it an offence for a relevant institution, (which are defined, but include deposit taking institutions), to fail to notify the Governor if the institution becomes aware, or suspects, a customer is a listed person or has committed an offence specified in the Order.
- 5.307 **The Al-Qa’ida and Taliban (United Nations Measures) (Overseas Territories) Order 2002** was amended by **The Al-Qa’ida and Taliban (United Nations Measures) (Overseas Territories) (Amendment) Order 2002**, which amended the definition of relevant institution, however deposit taking institutions remain affected by the Order. It also contained a small number of technical amendments.
- 5.308 It should be appreciated that any obligations that arise under these Orders are in addition to any obligations under the AML/ATF suite of legislation and are separate from those obligations.
- 5.309 The list referred to in paragraph 5.306 can be located at the link provided below. Institutions should check against the list to ensure their obligations under the Orders are being fully complied with.

[The Al-Qaida and Taliban Sanctions Committee - 1267](#)

- 5.310 The European Union and the United Kingdom are also able to designate persons and entities as being subject to financial sanctions and in the United Kingdom the financial sanctions regime applies to all

institutions. AML/ATF regulated institutions doing business in other countries will need to be aware of the scope of relevant financial sanctions regimes in those countries.

- 5.311 The links provided below may be of assistance in relation to financial sanctions regimes in the United Kingdom, the European Union and the United States –

United Kingdom – HM Treasury:

[Financial sanctions - HM Treasury](#)

European Union – External Relations:

[Common Foreign & Security Policy \(CFSP\) - Sanctions or restrictive measures in force](#)

United States of America – Office of Foreign Asset Control:

[U.S. Treasury - Office of Foreign Assets Control](#)

- 5.312 A link is also provided to the United Kingdom Office of Public Sector Information where the statutory instruments, discussed in this section of the guidance notes, can be viewed and read.

[UK Statutory Instruments and Explanatory Memorandum](#)

Statutory Instrument No. 3366/2001 - The Terrorism (United Nations Measures) (Overseas Territories) Order 2001

Statutory Instrument No. 112/2002 - The Al-Qa'ida and Taliban (United Nations Measures) (Overseas Territories) Order 2002

Statutory Instrument No. 266/2002 - The Al-Qa'ida and Taliban (United Nations Measures) (Overseas Territories) (Amendment) Order 2002

ANNEX 5-I

CONFIRMATION OF VERIFICATION OF IDENTITY

PRIVATE INDIVIDUAL

INTRODUCTION BY A BERMUDA AML/ATF REGULATED FINANCIAL INSTITUTION

1: DETAILS OF INDIVIDUAL (see explanatory notes below)

Full name of Customer:			
Current Address:			
Previous address if address has changed in the last three months:			
Date of Birth:			

2: CONFIRMATION

We confirm that

- (a) the information in section 1 above was obtained by us in relation to the customer;
- (b) the evidence we have obtained to verify the identity of the customer meets the requirements of the Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing) Regulations 2008, and any relevant authoritative guidance provided in relation to the type of business or transaction to which this confirmation relates;
- (c) in the event of any enquiry from you, copies of the relevant customer records will be made available, to the extent that we are required under Bermuda law to retain these records.

Signed:	
Name:	
Position:	
Date:	

3: DETAILS OF INTRODUCING FIRM

Name of Licensed Entity:	
Jurisdiction:	
Name of Regulator:	
Regulator Reference No:	

Explanatory notes

- 1: A separate confirmation must be completed for each customer and where a third party is involved, the identity of that person must also be verified, and a confirmation provided.
- 2: This form cannot be used to verify the identity of any customer whose identity has not been verified as a result of being an existing client of the introducing firm prior to the introduction of the requirement for such verification - 1st January 2009.

ANNEX 5-II

CONFIRMATION OF VERIFICATION OF IDENTITY

PRIVATE INDIVIDUAL

**INTRODUCTION BY A FINANCIAL INSTITUTION LOCATED IN
A COUNTRY OR TERRITORY OTHER THAN BERMUDA
(which the receiving firm has accepted as being from an equivalent jurisdiction)**

1: DETAILS OF INDIVIDUAL (see explanatory notes below)

Full name of Customer:		
Current Address:		
Previous address if address has changed in the last three months:		
Date of Birth:		

2: CONFIRMATION

We confirm that:

- (a) the information in section 1 above was obtained by us in relation to the customer;
- (b) the evidence we have obtained to verify the identity of the customer meets the requirements of local law and regulation;
- (c) where the underlying evidence taken in relation to the verification of the customer's identity is held outside Bermuda, in the event of any enquiry from you, copies of the relevant customer records will be made available, to the extent that we are required under Bermuda law to retain these records.

Signed:	
Name:	
Position:	
Date:	

3: DETAILS OF INTRODUCING FIRM

Name of Licensed Entity:	
Jurisdiction:	
Name of Regulator:	
Regulator License No:	

Explanatory notes

- 1: A separate confirmation must be completed for each customer and where a third party is involved, the identity of that person must also be verified, and a confirmation provided.
- 2: This form cannot be used to verify the identity of any customer whose identity has not been verified as a result of being an existing client of the introducing firm prior to the introduction of the requirement for such verification - 1st January 2009.

ANNEX 5-III

**CONFIRMATION OF VERIFICATION OF IDENTITY
CORPORATE AND OTHER NON-PERSONAL ENTITY
INTRODUCTION BY A BERMUDA AML/ATF REGULATED FINANCIAL INSTITUTION**

1: DETAILS OF CUSTOMER (see explanatory notes below) * And dates of birth if known

Full name of Customer:	
Type of Entity (corporate, trust, etc):	
Location of Business (full operating address):	
Registered office in country of incorporation:	
Registered number (if applicable):	
Relevant company registry or market listing authority:	
Names* of directors (or equivalent):	
Names* of beneficial owners (over 25%):	

2: CONFIRMATION

We confirm that

- (a) the information in section 1 above was obtained by us in relation to the customer;
- (b) the evidence we have obtained to verify the identity of the customer meets the requirements of the Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing) Regulations 2008, and any relevant authoritative guidance provided in relation to the type of business or transaction to which this confirmation relates;
- (c) in the event of any enquiry from you, copies of the relevant customer records will be made available, to the extent that we are required under Bermuda law to retain these records.

Signed:	
Name:	
Position:	
Date:	

3: DETAILS OF INTRODUCING FIRM

Name of Licensed Entity:	
Business Address:	
Name of Regulator:	
Regulator Reference No:	

Explanatory notes

- 1: "Relevant company registry" includes other registers, such as those maintained by charity commissions (or equivalent) or chambers of commerce.
- 2: This form cannot be used to verify the identity of any customer whose identity has not been verified as a result of being an existing client of the introducing firm prior to the introduction of the requirement for such verification - 1st January 2009.

ANNEX 5-IV

**CONFIRMATION OF VERIFICATION OF IDENTITY
CORPORATE AND OTHER NON-PERSONAL ENTITY**

**INTRODUCTION BY A FINANCIAL INSTITUTION LOCATED
IN A COUNTRY OR TERRITORY OTHER THAN BERMUDA**

1: DETAILS OF CUSTOMER (see explanatory notes below) * And dates of birth if known

Full name of Customer:	
Type of Entity (corporate, trust, etc):	
Location of Business (full operating address):	
Registered office in country of incorporation:	
Registered number (if applicable):	
Relevant company registry or market listing authority:	
Names* of directors (or equivalent):	
Names* of beneficial owners (over 25%):	

2: CONFIRMATION

We confirm that

- (a) the information in section 1 above was obtained by us in relation to the customer;
- (b) the evidence we have obtained to verify the identity of the customer meets the requirements of local law and regulation;
- (c) where the underlying evidence taken in relation to the verification of the customer's identity is held outside Bermuda, in the event of any enquiry from you, copies of the relevant customer records will be made available, to the extent that we are required under Bermuda law to retain these records.

Signed:	
Name:	
Position:	
Date:	

3: DETAILS OF INTRODUCING FIRM

Name of Licensed Entity:	
Business Address:	
Name of Regulator:	
Regulator Reference No:	

Explanatory notes

- 1: "Relevant company registry" includes other registers, such as those maintained by charity commissions (or equivalent) or chambers of commerce.
- 2: This form cannot be used to verify the identity of any customer whose identity has not been verified as a result of being an existing client of the introducing firm prior to the introduction of the requirement for such verification - 1st January 2009.

ANNEX 5-V

**CONFIRMATION OF VERIFICATION OF IDENTITY
GROUP INTRODUCTION**

PRIVATE INDIVIDUAL

1: DETAILS OF INDIVIDUAL (see explanatory notes below)

Full name of Customer:		
Current Address:		
Previous address if address has changed in the last three months:		
Date of Birth:		

2: CONFIRMATION

We confirm that

- (a) the verification of the identity of the above customer meets the requirements:
- i. of the Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing) Regulations 2008 and the guidance for standard evidence set out within the guidance issued by the Bermuda Monetary Authority; or
 - ii. of local law and regulation, and any relevant authoritative guidance provided in relation to the type of business or transaction to which this confirmation relates; or
- (b) where the underlying evidence taken in relation to the verification of the customer's identity is held outside Bermuda, in the event of any enquiry from you, copies of the relevant customer records will be made available, to the extent that we are required under Bermuda law to retain these records.

Signed:	
Name:	
Position:	
Date:	

3: DETAILS OF GROUP FIRM

Name of Licensed entity:	
Relationship to receiving entity:	
Business address:	
Jurisdiction:	
Registered number (if applicable):	

Explanatory notes

- 1: A separate confirmation must be completed for each customer and where a third party is involved, the identity of that person must also be verified, and a confirmation provided
- 2: This form cannot be used to verify the identity of any customer whose identity has not been verified as a result of being an existing client of the introducing firm prior to the introduction of the requirement for such verification - 1st January 2009.

ANNEX 5-VI

**CONFIRMATION OF VERIFICATION OF IDENTITY - GROUP INTRODUCTION
CORPORATE AND OTHER NON-PERSONAL ENTITY**

1: DETAILS OF CUSTOMER (see explanatory notes below) * And dates of birth if known

Full name of Customer:	
Type of Entity (corporate, trust, etc):	
Location of Business (full operating address):	
Registered office in country of incorporation:	
Registered number (if applicable):	
Relevant company registry or market listing authority:	
Names* of directors (or equivalent):	
Names* of beneficial owners (over 25%):	

2: CONFIRMATION

We confirm that

- (a) the verification of the identity of the above customer meets the requirements:
- i. of the Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing) Regulations 2008 and the guidance for standard evidence set out within the guidance issued by the Bermuda Monetary Authority; or
 - ii. of local law and regulation, and any relevant authoritative guidance provided in relation to the type of business or transaction to which this confirmation relates; or
- (b) where the underlying evidence taken in relation to the verification of the customer's identity is held outside Bermuda, in the event of any enquiry from you, copies of the relevant customer records will be made available, to the extent that we are required under Bermuda law to retain these records.

Signed:	
Name:	
Position:	
Date:	

3: DETAILS OF GROUP FIRM

Name of Licensed entity:	
Relationship to receiving entity:	
Jurisdiction:	
Name of regulator:	
Registered number (if applicable):	

Explanatory notes

- 1: "Relevant company registry" includes other registers, such as those maintained by charity commissions (or equivalent) or chambers of commerce.
- 2: This form cannot be used to verify the identity of any customer whose identity has not been verified as a result of being an existing client of the introducing firm prior to the introduction of the requirement for such verification - 1st January 2009.

CHAPTER 6

SUSPICIOUS ACTIVITY REPORTING

Relevant law/regulation

Regulation 16 & Regulation 17
POCA S46
ATFA Schedule 1

Core obligations

- Staff of an institution must raise an internal report where they have knowledge or suspicion, that another person is engaged in money laundering, or terrorist financing.
- The institution's reporting officer must consider all internal reports.
- The institution's reporting officer must make an external report to the Financial Intelligence Agency as soon as is practicable if he considers that there is knowledge or suspicion that another person is engaged in money laundering, or terrorist financing.
- Institutions are required not to make any funds available to any person specified, in written notice received from the Financial Intelligence Agency, for a period not exceeding 72 hours. Financial Intelligence Agency Act 2007 S. 15(1).
- It is a criminal offence for any person who knows or suspects that a disclosure has been made to the Financial Intelligence Agency or a reporting officer, to disclose to any person information in relation to such disclosure or to disclose information or any other matter which is likely to prejudice any investigation which might be conducted following such a disclosure.

Actions required, to be kept under regular review

- Enquiries made in respect of disclosures must be documented.
- The reasons why a Suspicious Activity Report (SAR) was, or was not, forwarded to the Financial Intelligence Agency should be recorded.
- Any communications made with or received from the authorities, including the Financial Intelligence Agency, in relation to a SAR should be maintained on file.

General legal and regulatory obligations

POCA S46
ATFA Schedule 1

6.1 Persons are required to make a report in respect of information or any other matter that comes to them in the course of their trade, profession, business or employment:

- Where they know; or
- Where they suspect

that a person is engaged in money laundering or terrorist financing.

Regulation 16(2)(d), 17 & 18

6.2 In order to provide a framework within which suspicious activity reports may be raised and considered:

- Each institution must ensure that any member of staff, reports to the institution's reporting officer, where they have a knowledge or suspicion that a person or customer is engaged in money laundering or terrorist financing;
- The institution's reporting officer must consider each such report, and determine whether it gives rise to such a knowledge or suspicion; and

- Institutions should ensure that staff are appropriately trained in their obligations, and in the requirements for making reports to their reporting officer.

POCA S46 & ATFA Schedule 1

- 6.3 If the reporting officer determines that a report does give rise to a knowledge or suspicion, he must report that knowledge or suspicion to the Financial Intelligence Agency. Under POCA, the reporting officer is required to make a report to the Financial Intelligence Agency as soon as is reasonably practicable if he knows or suspects that another person is engaged in money laundering. Under the ATFA, similar conditions apply in relation to disclosure where there are grounds for suspicion of terrorist financing.
- 6.4 A sole trader with no employees who knows or suspects that a customer of his, or the person on whose behalf the customer is acting, is or has been engaged in money laundering or terrorist financing, must make a report as soon as is reasonably practicable to the Financial Intelligence Agency.

What is meant by “knowledge” and “suspicion”?

POCA, S. 46 & ATFA Schedule 1

- 6.5 Having knowledge means knowing the existence of certain facts. In a criminal court, it must be proved that the individual in fact knew that a person was engaged in money laundering. That said, knowledge can be inferred from the surrounding circumstances; so, for example, a failure to ask obvious questions may be relied upon by a jury to imply knowledge. The knowledge must, however, have come to the person in the course of their trade, profession, business or employment. Information that comes to the person in other circumstances does not come within the scope of S. 46 of POCA or Schedule 1 of the ATFA and therefore no obligation exists to make a report. This does not preclude a report being made should the person choose to do so.
- 6.6 Suspicion is more subjective and falls short of proof based on firm evidence. Suspicion has been defined by the courts as being beyond mere speculation and based on some foundation, for example: **“A degree of satisfaction and not necessarily amounting to belief but at least extending beyond speculation as to whether an event has occurred or not”**; and **“Although the creation of suspicion requires a lesser factual basis than the creation of a belief, it must nonetheless be built upon some foundation.”** Justice Nelson in the case of *N2J Ltd v Cater Allen* before the High Court in London cited with approval Lord Devlin’s definition of suspicion in *Hussein v Chong Fook Kam* [1970] AC 942: **“Suspicion in its ordinary meaning is a state of conjecture or surmise where proof is lacking.”** **“I suspect but I cannot prove.”** Justice Nelson continued **“Suspicion does not have to have a long history of misdoing before it arises. It may arise in an otherwise seamless period of good conduct from one important new piece of information.”** **“Suspicion may be no more than a feeling based on material which may fall well short of prima facie evidence.”**
- 6.7 A transaction which appears unusual is not necessarily suspicious. Even customers with a stable and predictable transactions profile will have periodic transactions that are unusual for them. Many customers will, for perfectly good reasons, have an erratic pattern of transactions or account activity. So the unusual is, in the first instance, only a basis for further enquiry, which may in turn require judgement as to whether it is suspicious. A transaction or activity may not be suspicious at the time, but if suspicions are raised later, an obligation to report then arises.
- 6.8 A member of staff, including the reporting officer, who considers a transaction or activity to be suspicious, would not necessarily be expected either to know or to establish the exact nature of any underlying criminal offence, or that the particular funds or property were definitely those arising from a crime or terrorist financing.
- 6.9 Transactions, or proposed transactions, as part of ‘419’ scams are attempted advance fee frauds, and not money laundering; they are therefore not reportable under POCA or the ATFA, unless the fraud is successful, and the institution is aware of resulting criminal property being laundered.

Internal reporting

Regulation 16(2)(d)(i) & 17 and POCA S46 and ATFA Schedule 1

- 6.10 The obligation to report to the reporting officer within the institution where they have a knowledge or suspicion of money laundering or terrorist financing is placed on all employees. All institutions therefore need to ensure that all employees know who they should report suspicions to.
- 6.11 Institutions may wish to set up internal systems that allow staff to consult with their line manager before sending a report to the reporting officer. The obligation under POCA is to report 'as soon as is reasonable', and so any such consultations should take this into account. Where an institution sets up such systems it should ensure that they are not used to prevent reports reaching the reporting officer whenever staff have stated that they have knowledge or suspicion that a transaction or activity may involve money laundering or terrorist financing.
- 6.12 Whether or not a member of staff consults colleagues, the legal obligation remains with the staff member to decide for himself whether a report should be made; he must not allow colleagues to decide for him. Where a colleague has been consulted, he himself will then have knowledge on the basis of which he must consider whether a report to the reporting officer is necessary. In such circumstances, institutions should make arrangements such that the reporting officer only receives one report in respect of the same information giving rise to knowledge or suspicion.
- 6.13 Short reporting lines, with a minimum number of people between the person with the knowledge or suspicion and the reporting officer, will ensure speed, confidentiality and swift access to the reporting officer.
- 6.14 All suspicions reported to the reporting officer should be documented, or recorded electronically. The report should include full details of the customer who is the subject of concern and as full a statement as possible of the information giving rise to the knowledge or suspicion. All internal enquiries made in relation to the report should also be documented, or recorded electronically. This information may be required to supplement the initial report or as evidence of good practice and best endeavours if, at some future date, there is an investigation and the suspicions are confirmed or disproved.
- 6.15 Once an employee has reported his suspicion in an appropriate manner to the reporting officer, or to an individual to whom the reporting officer has delegated the responsibility to receive such internal reports, he has fully satisfied his statutory obligation.
- 6.16 Until the reporting officer advises the member of staff making an internal report that no report to the Financial Intelligence Agency is to be made, further transactions or activity in respect of that customer, whether of the same nature or different from that giving rise to the previous suspicion, should be reported to the reporting officer as they arise.

Non-Bermuda offences

POCA S45(B)

- 6.17 The offence of money laundering, and the duty to report under POCA, apply in relation to the proceeds of any criminal conduct, wherever carried out, that would constitute an offence if it took place in Bermuda. This broad scope excludes offences which the institution, staff member or reporting officer knows, or believes on reasonable grounds, to have been committed in a country or territory other than Bermuda and not to be unlawful under the criminal law then applying in the country or territory concerned.

ATFA S17

- 6.18 The duty to report under the ATFA applies in relation to any terrorist financing offence under S5-8 of that Act, that would have been an offence under these sections of the Act had it occurred in Bermuda.

Evaluation and determination by the reporting officer

Regulation 16(2)(d) & Regulation 17

- 6.19 The institution's reporting officer must consider each report and determine whether it gives rise to knowledge or suspicion that a person is engaged in money laundering or terrorist financing. The institution must permit the reporting officer to have access to any information, including CDD information, in the institution's possession which could be relevant. The reporting officer may also require further information to be obtained, from the customer if necessary, or from an intermediary who introduced the customer to the institution, to the extent that the introducer still holds the information (bearing in mind his own record keeping requirements). Any approach to the customer or to the intermediary should be made sensitively, and probably by someone other than the reporting officer, to minimize the risk of alerting the customer or an intermediary that a disclosure to the Financial Intelligence Agency may be being considered.
- 6.20 When considering an internal suspicious activity report, the reporting officer, taking account of the risk posed by the transaction or activity being addressed, will need to strike the appropriate balance between the requirement to make a timely disclosure to the Financial Intelligence Agency, and any delays that might arise in searching a number of unlinked systems and records that might hold relevant information.
- 6.21 As part of the review, other known connected accounts or relationships may need to be examined. Connectivity can arise commercially (through linked accounts, introducers, etc.), or through individuals (third parties, controllers, signatories etc.). Given the need for timely reporting, it may be prudent for the reporting officer to consider making an initial report to the Financial Intelligence Agency prior to completing a full review of linked or connected relationships, which may or may not subsequently need to be reported.
- 6.22 If the reporting officer decides not to make a report to the Financial Intelligence Agency, the reasons for not doing so should be clearly documented, or recorded electronically, and retained with the internal suspicious activity report.

External reporting

Regulation 16(2)(d) and Regulation 17 & POCA S46 & ATFA Schedule 1

- 6.23 The institution's reporting officer must report to the Financial Intelligence Agency any transaction or activity that, after his evaluation, he knows or suspects to be linked to money laundering or terrorist financing. Such reports must be made as soon as is reasonably practicable after the information comes to him.
- 6.24 In order that an informed overview of the situation may be maintained, all contact between particular departments/branches and the Financial Intelligence Agency or law enforcement should be controlled through, or reported back to a single contact point, which will typically be the reporting officer. In the alternative, it may be appropriate to route communications through an appropriate member of staff in the institution's legal or compliance department.
- 6.25 A SAR's intelligence value is related to the quality of information it contains. An institution needs to have good base data from which to draw the information to be included in the SAR; there needs to be a system to enable all the relevant information to be produced in hard copy for the Financial Intelligence Agency, or law enforcement if requested under a court order.
- 6.26 Institutions should include in each SAR as much relevant information about the customer, transaction or activity as it has in its records. The Financial Intelligence Agency's website at www.fia.bm contains guidance on completing SARs in a way that gives most assistance and provides a link to a SAR template.

Where to report

- 6.27 To avoid committing a failure to report offence, reporting officers must make their disclosures to the Financial Intelligence Agency, the central reception point for disclosure of suspicions and, if appropriate, for providing consent to continue to proceed with the transaction or activity.
- 6.28 The Financial Intelligence Agency is located at 6th Floor, Strata 'G' Building, 30A Church Street, Hamilton HM11 and it can be contacted during office hours on telephone number (441)-292-3422 or fax number (441)-296-3422 or email at info@fia.bm

Attempted fraud and attempted money laundering

POCA S. 46

- 6.29 POCA provides that a disclosure must be made where there is a knowledge or suspicion that a person is engaged in money laundering. "Money laundering" is defined in POCA to include an attempt to commit an offence under S43, 44 or 45. There is no duty under S 46 to disclose information about unsuccessful attempts to commit fraud or other non-money laundering offences. However, as soon as the institution knows or suspects that any benefit has been acquired arising from criminal activity, whether by a fraudster himself or by any third party, so that there is the proceeds of criminal conduct in existence, then, any knowledge or suspicion of money laundering or terrorist financing must be reported to the Financial Intelligence Agency.

Penalties

POCA S46 & ATFA Schedule 1

- 6.30 Where a person fails to comply with the obligation under POCA or the ATFA to make disclosures to a reporting officer and/or to the Financial Intelligence Agency as soon as is reasonably practicable after the information giving rise to the knowledge or suspicion comes to the attention of the member of staff, that person may be liable to criminal prosecution. The criminal sanction, under POCA or the ATFA, is a prison term of up to three years on summary conviction or ten years on conviction in indictment and/or a fine.

Consent

POCA S44(3)(b)(i) & 45(5)(b)(i)

- 6.31 Care should be taken, when a disclosure is made prior to a transaction being completed that the disclosure does not lead to the unnecessary freezing of a customer's account, thus affecting other, non-suspicious transactions.

Consent under POCA

POCA S. 44(3)(b)(i) & 45(5)(b)(i)

- 6.32 Reporting before or reporting after the event are not equal options which a person can choose between. Where a customer instruction is received prior to a transaction or activity taking place, or arrangements being put in place, and there is a knowledge or suspicion that the transaction, arrangements, or the funds/property involved, relate to money laundering or terrorist financing, a report must be made to the Financial Intelligence Agency. In such circumstances it would be prudent to seek consent from the Financial Intelligence Agency to proceed with that transaction or activity and where consent is not forthcoming, establish what information can be provided to the customer.

POCA S44(3)(b)(ii) & S45(5)(b)(ii)

- 6.33 When an activity or transaction (or a related transaction), which gives rise to a knowledge or suspicion of money laundering, has been completed the person does not commit an offence if after doing the act and on his own initiative he makes a disclosure as soon as it is reasonable for him to make it.
- 6.34 Consent can only apply where there is prior notice to the Financial Intelligence Agency of the transaction or activity. The Financial Intelligence Agency cannot provide consent after the transaction or activity has occurred.

Consent under ATFA S12

- 6.35 A person does not commit an offence under sections 5-8 of the AT(FOM)A if he acts in accordance with the express consent of the Financial Intelligence Agency.

Tipping Off

POCA S47 & ATFA S10A

- 6.36 POCA & ATFA contain sections creating offences of “tipping off”

POCA S47(1) & ATFA S10A(1)

- 6.37 Where a person knows or suspects that the police are acting or proposing to act in connection with an investigation which is being or is about to be conducted into money laundering or terrorist financing, and discloses any information to any other person which is likely to prejudice that investigation or proposed investigation, they commit an offence. It is a defence if the person does not know or suspect that disclosure is likely to prejudice the investigation.

POCA S47(2) & ATFA S10A(2)

- 6.38 Once an internal or external suspicious activity report has been made, it is a criminal offence for any person knowing or suspecting that such a report has been made, to disclose to any other person information or any other matter which is likely to prejudice any investigation which might be conducted following such a disclosure.
- 6.39 Reasonable enquiries of a customer, conducted in a tactful manner, regarding the background to a transaction or activity that is inconsistent with the normal pattern of activity is prudent practice, forms an integral part of customer due diligence measures, and should not give rise to tipping off.
- 6.40 The fact that a transaction or activity is notified to the Financial Intelligence Agency before the event, and the Financial Intelligence Agency provides consent to continue with the transaction or activity, does not alter the position so far as ‘tipping off’ is concerned.
- 6.41 This means that an institution:
- Cannot, at the time, tell a customer that a transaction is being delayed because a report has been made to the Financial Intelligence Agency;
 - Cannot tell a customer that a transaction is being delayed because the institution has received notice not to make funds available to any person by virtue of the Financial Intelligence Agency Act 2007, section 15(1); and
 - Cannot tell the customer that law enforcement is conducting an investigation.

Transactions following a disclosure

- 6.42 Institutions must remain vigilant for any additional transactions by, or instructions from, any customer or account in respect of which a disclosure has been made, and should submit further disclosures, to the Financial Intelligence Agency, as appropriate.

POCA S 44(3)(a) & 45(5)(a) & 46(1) and ATFA Schedule 1

- 6.43 The disclosure provisions within POCA and the ATFA protect persons making SARs from any potential breaches of confidentiality, however imposed. These provisions apply to any person who makes a report and includes reports that are made voluntarily, in addition to reports made in order to fulfill reporting obligations.
- 6.44 The Financial Intelligence Agency's consent following a disclosure, is given to the reporting institution solely in relation to money laundering or terrorist financing offences. Consent provides the staff involved with a defence against a charge of committing a money laundering or terrorist financing offence under S. 44 & 45 of POCA or S. 5, 6, 7 & 8 of ATFA. It is not intended to override normal commercial judgement, and an institution is not committed to continuing the relationship with the customer if such action would place the reporting institution at commercial risk.
- 6.45 Whether to terminate a relationship is essentially a commercial decision, and institutions must be free to make such judgements. However, in the circumstances envisaged here an institution should consider liaising with the Financial Intelligence Agency to consider whether it is likely that termination would alert the customer or prejudice an investigation in any other way. If there is continuing suspicion about the customer or the transaction or activities, and there are funds which need to be returned to the customer at the end of the relationship, institutions should seek guidance from the Financial Intelligence Agency before repatriating the funds.

Constructive trusts

- 6.46 The duty to report suspicious activity and to avoid tipping off could, in certain circumstances, lead to a potential conflict between the reporting institution's responsibilities under the criminal law and its obligations under the civil law, as a constructive trustee, to a victim of a fraud or other crimes.
- 6.47 An institution's liability as a constructive trustee under Bermuda law can arise when it either knows that the funds held by the institution do not belong to its customer, or is on notice that such funds may not belong to its customer. The institution will then take on the obligation of a constructive trustee for the rightful owner of the funds. If the institution pays the money away other than to the rightful owner, and it is deemed to have acted dishonestly in doing so, it may be held liable for knowingly assisting a breach of trust.
- 6.48 Having a suspicion that it considers necessary to report under the money laundering or terrorist financing legislation may, in certain circumstances, indicate that the institution knows that the funds do not belong to its customer, or is on notice that they may not belong to its customer. However, such suspicion may not itself be enough to cause an institution to become a constructive trustee. Case law suggests that a constructive trust will only arise when there is some evidence that the funds belong to someone other than the customer.
- 6.49 If, when making a suspicious activity report, an institution knows that the funds which are the subject of the report do not belong to its customer, or has doubts that they do, this fact, and details of the institution's proposed course of action, should form part of the report that is forwarded to the Financial Intelligence Agency.
- 6.50 If the customer wishes subsequently to withdraw or transfer the funds, the institution should, in the first instance, contact the Financial Intelligence Agency for guidance. If consent is granted for the withdrawal or transfer of funds this however, may not necessarily protect the institution from the risk of committing a breach of constructive trust by transferring the funds. In situations where the assistance of the court is necessary, it is open to an institution to apply to the court for directions as to whether the customer's

request should be met. However, the powers of the court are discretionary, and should only be used in cases of real need. That said, it is unlikely that an institution acting upon the direction of a court would later be held to have acted dishonestly such as to incur liability for breach of constructive trust.

- 6.51 Although each case must be considered on its facts, the effective use of customer information, and the identification of appropriate underlying beneficial owners, can help institutions to guard against a potential constructive trust suit arising out of fraudulent misuse or misappropriation of funds.

Additional reporting obligations on Relevant Institutions

- 6.52 In addition to the reporting obligations outlined in this chapter, institutions should be aware of the reporting requirements under the Terrorism (United Nations Measures) (Overseas Territories) Order 2001 and the Al-Qa'ida and Taliban (United Nations Measures) (Overseas Territories) Order 2002 whereby relevant institutions, under certain circumstances, have an obligation to make reports to the Governor. These obligations are explained in greater detail at paragraph 5.304 – 5.312.

CHAPTER 7

STAFF TRAINING AND AWARENESS

Relevant law/regulation

Regulation 18

Core obligations

Relevant employees should be:

- Made aware of the risks of money laundering and terrorist financing, the relevant legislation, and their obligations under that legislation;
- Made aware of the identity and responsibilities of the institution's reporting officer; and
- Trained in the institution's procedures and in how to recognise and deal with potential money laundering or terrorist financing transactions or activity.

Staff training should be given at regular intervals, and details recorded.

Actions required, to be kept under regular review

- Provide appropriate training to make relevant employees aware of money laundering and terrorist financing issues, including how these crimes operate and how they might take place through the institution.
- Ensure that relevant employees are provided with information on, and understand, the legal position of the institution and of individual members of staff, and of changes to these legal positions.
- Consider providing relevant employees with case studies and examples related to the institution's business.
- Train relevant employees in how to operate a risk-based approach to AML/ATF.

Why focus on staff awareness and training?

- 7.1 One of the most important controls over the prevention and detection of money laundering or terrorist financing is to have staff that are alert to the risks of money laundering/terrorist financing and well trained in the identification of unusual activities or transactions which may prove to be suspicious.
- 7.2 The effective application of even the best designed control systems can be quickly compromised if the staff applying the systems are not adequately trained. The effectiveness of the training will therefore be important to the success of the institution's AML/ATF strategy.
- 7.3 It is essential that institutions implement a clear and well articulated policy for ensuring that relevant employees are aware of their obligations in respect of the prevention of money laundering and terrorist financing and for training them in the identification and reporting of anything that gives grounds for suspicion. This is especially important for staff who handle customer transactions or instructions. Temporary and contract staff carrying out such functions should also be covered by these training programmes.

POCA S43-45 & S46 and ATFA S8

- 7.4 Under POCA and the ATFA, individual members of staff face criminal penalties if they are involved in money laundering or terrorist financing, or if they do not report their knowledge or suspicion of money laundering or terrorist financing. It is important, therefore, that staff are made aware of these obligations, and are given training in how to discharge them.

General legal and regulatory obligations

Regulation 16

- 7.5 The obligations on senior management and the institution in relation to staff awareness and staff training address each requirement separately. The Regulations require institutions to take appropriate measures so that all relevant employees are made aware of the law relating to money laundering and terrorist financing, and that they are regularly given training in how to recognise and deal with transactions which may be related to money laundering or terrorist financing.
- 7.6 Senior management should have responsibility for oversight of the institution's AML/ATF systems and controls, which include appropriate training for the institution's employees in relation to money laundering.

Regulation 18

- 7.7 Institutions are liable to civil penalties for not having adequate training and awareness arrangements in place, therefore institutions should not only obtain acknowledgement from the individual that they have received the necessary training, but should also take steps to assess its effectiveness.

Responsibilities of senior management

Regulation 16

- 7.8 Senior management should be aware of their obligations under the Regulations to establish appropriate systems and procedures to forestall and prevent operations relating to money laundering and terrorist financing. It is a breach of the Regulations not to have appropriate systems in place, whether or not money laundering or terrorist financing has taken place.

Regulation 16

- 7.9 As noted in paragraph 1.23, the relationship between the reporting officer and the director(s)/senior manager(s) allocated overall responsibility for the establishment and maintenance of the institution's AML/ATF systems (where they are not the same person) is one of the keys to a successful AML/ATF regime. It is important that this relationship is clearly defined and documented, so that each knows the extent of his, and the other's, role and day-to-day responsibilities.
- 7.10 Institutions should take reasonable steps to ensure that relevant employees are aware of:
- Their responsibilities under the institution's arrangements for the prevention of money laundering and terrorist financing, including those for obtaining sufficient evidence of identity, recognising and reporting knowledge or suspicion of money laundering or terrorist financing;
 - The identity and responsibilities of the reporting officer; and
 - The potential effect on the institution, on its employees personally and on its clients, of any breach of that law.
- 7.11 The institution's approach to training should be built around ensuring that the content and frequency of training reflects the risk assessment of the products and services of the institution and the specific role of the individual.

Responsibilities of staff

- 7.12 Staff should be made aware of their personal responsibilities and those of the institution at the start of their employment. These responsibilities should be documented in such a way as to enable staff to refer to them as and when appropriate throughout their employment. In addition, selected or relevant employees should be given regular and appropriate training in order to be aware of:
- The criminal law relating to money laundering and terrorist financing;

- The Regulations;
- Supervisory guidance;
- The risks money laundering and terrorist financing pose to the business;
- The vulnerabilities of the institution's products and services; and
- The institution's policies and procedures in relation to the prevention of money laundering and terrorist financing.

7.13 Where staff move between jobs, or change responsibilities, their training needs may change. On-going training should be given at appropriate intervals to all relevant employees.

Legal obligations on staff

POCA S43-45 & S46 & S47 and ATFA S5-8

7.14 There are several offences under POCA and the ATFA which directly affect staff – the various offences of money laundering or terrorist financing, failure to report a knowledge or suspicion of money laundering or terrorist financing, tipping off and disclosure of information.

7.15 These offences apply to all staff and have no particular application to those engaged in specific customer related activities – that is, they also apply to “back office” staff.

POCA S46 & S47

7.16 Once a report has been made to the Financial Intelligence Agency or the institution's reporting officer, it is an offence for any person to disclose to any other person information in relation to such disclosure or to disclose to any other person information or other matter likely to prejudice an investigation.

Training in the institution's procedures

7.17 The institution should train staff, in particular, on how its products and services may be used as a vehicle for money laundering or terrorist financing, and in the institution's procedures for managing this risk. They will also need information on how the institution may itself be at risk of prosecution for money laundering.

7.18 Relevant employees should be trained in what they need to know in order to carry out their particular role. Staff involved in customer acceptance, in customer servicing, or in settlement functions will need different training, tailored to their particular function. This may involve making them aware of the importance of the “CDD” requirements for money laundering and terrorist financing prevention purposes, and of the respective importance of customer identification procedures, obtaining additional information and monitoring customer activity. The awareness raising and training in this respect should cover the need to verify the identity of the customer, and circumstances when it should be necessary to obtain appropriate additional customer information in the context of the nature of the transaction or business relationship concerned.

7.19 Relevant employees should also be made aware of the particular circumstances of customers who present a higher-risk of money laundering or terrorist financing. Training should include how identity should be verified in such cases, what additional steps should be taken, and/or what local checks can be made.

Staff alertness to specific situations

7.20 Sufficient training will need to be given to all relevant employees to enable them to recognise when a transaction is unusual or suspicious.

7.21 The set of circumstances giving rise to an unusual transaction or arrangement, and which may give rise to a knowledge or suspicion of money laundering or terrorist financing, will depend on the customer and the product or service in question. Illustrations of the type of situation that may be unusual, and which in certain circumstances might give rise to such knowledge or suspicion, are:

- Transactions which have no apparent purpose, or which make no obvious economic sense, or which involve apparently unnecessary complexity;
- The use of non-resident accounts, companies or structures in circumstances where the customer's needs do not appear to support such economic requirements;
- Where the transaction being requested by the customer, or the size or pattern of transactions, is, without reasonable explanation, out of the ordinary range of services normally requested or is inconsistent with the experience of the institution in relation to the particular customer;
- Dealing with customers not normally expected in that part of the business;
- Transfers to and from high-risk jurisdictions, without reasonable explanation, which are not consistent with the customer's declared foreign business dealings or interests;
- Where a series of transactions are structured just below the "occasional transaction" threshold to avoid CDD requirements;
- Where a customer who has entered into a business relationship with the institution uses the relationship for a single transaction or for only a very short period of time;
- Unnecessary routing of funds through third party accounts; and
- Unusual investment transactions without an apparently discernible profitable motive.

7.22 Issues around the customer identification process that may raise concerns include such matters as the following:

- Has the customer refused, or appeared particularly reluctant, to provide the information requested without reasonable explanation?
- Do you understand the legal and corporate structure of the client entity, and its ownership and control, and does the structure appear to make sense?
- Is the staff member aware of any inconsistencies between locations and other information provided?
- Is the area of residence given consistent with other profile details, such as employment?
- Does an address appear vague or unusual – e.g., an accommodation agency, a professional 'registered office' or a trading address?
- Does it make sense for the customer to be opening the account or relationship in the jurisdiction that he is asking for?
- Is the information that the customer has provided consistent with the banking or other services or facilities that he is seeking?
- Does the supporting documentation add validity to the other information provided by the customer?
- Does the customer have other banking or financial relationships with the institution, and does the collected information on all these relationships appear consistent?
- Does the client want to conclude arrangements unusually urgently, against a promise to provide information at a later stage, which is not satisfactorily explained?
- Has the customer suggested changes to a proposed arrangement in order to avoid providing certain information?

7.23 Staff should also be on the lookout for such things as:

- Sudden, substantial increases in cash deposits or levels of investment, without adequate explanation;
- Transactions made through other banks or institutions;
- Regular large, or unexplained, transfers to and from countries known for money laundering, terrorism, corruption or drug trafficking;
- Large numbers of electronic transfers into and out of the account;
- Significant/unusual/inconsistent deposits by third parties; and
- Reactivation of dormant account(s).

7.24 Staff awareness and training programmes may also include the nature of terrorism funding and terrorist activity, in order that staff are alert to customer transactions or activities that might be terrorist-related.

7.25 Examples of activity that might suggest to staff that there could be potential terrorist activity include:

- Round sum deposits, followed by like-amount wire transfers;
- Frequent international ATM activity;

- No known source of income;
- Use of wire transfers and the internet to move funds to and from high-risk countries and geographic locations;
- Frequent address changes;
- Purchases of military items or technology; and
- Media reports on suspected, arrested terrorists or groups.

- 7.26 It is important that staff are appropriately made aware of changing behaviour and practices amongst money launderers and those financing terrorism. As well as their regular series of publications on the typologies of financial crime, FATF's Guidance for Financial Institutions in Detecting Terrorist Financing issued in April 2002 contains an in-depth analysis of the methods used in the financing of terrorism and the types of financial activities constituting potential indicators of such activities. These documents are available at www.fatf-gafi.org.
- 7.27 The UK Serious Organized Crime Agency publishes a range of material at www.soca.gov.uk, such as threat assessments and risk profiles, of which institutions may wish to make their staff aware. The information on this website could usefully be incorporated into institutions' training materials.
- 7.28 Illustrations, based on real cases, of how individuals and organisations might raise funds and use financial sector products and services for money laundering or to finance terrorism, are available at www.jmlsg.org.uk.

Staff based in a Country or Territory Other than Bermuda

- 7.29 Where activities relating to Bermuda business operations are undertaken by staff in a country or territory other than Bermuda, those staff must be made aware of and trained to follow the AML/ATF policies and procedures applicable to the Bermuda operations. It is important that any local training and awareness obligations are also met, where relevant.

Training methods and assessment

- 7.30 There is no single solution when determining how to deliver training; a mix of training techniques may be appropriate. On line learning systems can often provide an adequate solution for many employees, but there will be classes of employees for whom such an approach is not suitable. Focused classroom training for higher-risk or minority areas can be more effective. Relevant videos always stimulate interest, but continually re-showing the same video may produce diminishing returns.
- 7.31 Procedures manuals, whether paper or intranet based, are useful in raising staff awareness and in supplementing more dedicated forms of training, but their main purpose is to provide on-going reference and they are not generally written as training material.
- 7.32 On-going training should be given at appropriate intervals to all relevant employees. Particularly in larger institutions, this may take the form of a rolling programme.
- 7.33 Whatever the approach to training, it is vital to establish comprehensive records (see paragraph 8.19) to monitor who has been trained, when they received the training, the nature of the training given and its effectiveness.

CHAPTER 8

RECORD KEEPING

Relevant law/regulation

Regulations 15 & 16

Core obligations

Institutions must retain:

- Copies of, or references to, the evidence they obtained of a customer's identity, for five years after the end of the customer relationship; and
- Details of customer transactions for five years from the date of the transaction.

Institutions should retain:

- Details of actions taken in respect of internal and external suspicious activity reports; and
- Details of information considered by the reporting officer in respect of an internal report where no external report is made.

Actions required, to be kept under regular review

- Institutions should maintain appropriate systems for retaining records.
- Institutions should maintain appropriate systems for making records available when required, within the specified timescales.

General legal and regulatory obligations

Regulation 15

- 8.1 This chapter provides guidance on appropriate record keeping procedures to meet an institution's obligations in respect of the prevention of money laundering and terrorist financing. There are general obligations on institutions to maintain appropriate records and controls more widely in relation to their business; this guidance is not intended to replace or interpret such wider obligations.
- 8.2 Record keeping is an essential component of the audit trail that the Regulations seek to establish in order to assist in any financial investigation and to ensure that criminal funds are kept out of the financial system, or if not, that they may be detected and confiscated by the authorities.

Regulation 15

- 8.3 Institutions must retain records concerning customer identification and transactions as evidence of the work they have undertaken in complying with their legal obligations, as well as for use as evidence in any investigation conducted by law enforcement.
- 8.4 Where an institution has relied on a third party it must ensure that that third party complies with the record keeping obligations under the Regulations.

What records have to be kept?

- 8.5 The precise nature of the records required is not specified in the Regulations. The objective is to ensure that an institution meets its obligations and that, in so far as is practicable, in any subsequent investigation the institution can provide the authorities with its section of the audit trail.

- 8.6 The institution's records should cover:
- Customer information;
 - Transactions;
 - Internal and external suspicious activity reports;
 - Compliance reports;
 - Information not acted upon;
 - Training and compliance monitoring; and
 - Information about the effectiveness of training.

Customer information

Regulation 15(2), (3) & (4)

- 8.7 In relation to the evidence of a customer's identity, institutions must keep a copy of, or the references to, the evidence of the customer's identity obtained during the application of customer due diligence measures. Where an institution has received a confirmation of identity certificate, this certificate will in practice be the evidence of identity that must be kept.
- 8.8 An institution may often hold additional information in respect of a customer obtained for the purposes of enhanced customer due diligence or on-going monitoring.
- 8.9 Where the individual presents himself to the institution, or at one of its branches, he may produce the necessary evidence of identity for the institution to take and retain copies.
- 8.10 Records of identification evidence must be kept for a period of at least five years after the relationship with the customer has ended except where a police officer has notified the institution in writing that particular records are or may be relevant to an investigation. Such records must then be kept pending the outcome of the investigation.
- 8.11 The date the relationship with the customer ends is the date:
- An occasional transaction, or the last in a series of linked transactions, is carried out; or
 - The business relationship ended, i.e. the closing of the account or accounts.
- 8.12 Where documents verifying the identity of a customer are held in one part of a group, they do not need to be held in duplicate form in another. The records do, however, need to be accessible to the reporting officer and to all areas that have contact with the customer, and be available on request, when these areas seek to rely on this evidence, or when they may be called upon by law enforcement to produce them.
- 8.13 When an introducing branch or subsidiary ceases to trade or have a business relationship with a customer, as long as his relationship with other group members continues, particular care needs to be taken to retain, or hand over, the appropriate customer records. Similar arrangements need to be made if a company holding relevant records ceases to be part of the group. This will also be an issue if the record keeping has been delegated to a third party.

Transactions

- 8.14 All transactions carried out on behalf of or with a customer in the course of relevant business must be recorded within the institution's records. Transaction records in support of entries in the accounts, in whatever form they are used, e.g. credit/debit slips, cheques, should be maintained in a form from which a satisfactory audit trail may be compiled where necessary, and which may establish a financial profile of any suspect account or customer.
- 8.15 Records of all transactions relating to a customer must be retained for a period of five years from the date on which the transaction is completed except where a police officer has notified the institution in writing

that particular records are or may be relevant to an investigation. Such records must be kept pending the outcome of the investigation.

Internal and external reports

- 8.16 An institution should make and retain:
- Records of actions taken under the internal and external reporting requirements; and
 - When the reporting officer has considered information or other material concerning possible money laundering or terrorist financing, but has not made a report to the Financial Intelligence Agency, a record of the other material that was considered.
- 8.17 In addition, copies of any SARs made to the Financial Intelligence Agency should be retained.
- 8.18 Records of all internal and external reports should be retained for five years from the date the report was made, except where the institution has been notified, in writing, by a police officer that particular records are or may be relevant to an investigation being carried out, these records must then be kept pending the outcome of the investigation.

Other records

- 8.19 An institution's records should include:
- (a) in relation to training:
- Dates AML training was given;
 - The nature of the training;
 - The name(s) of the person(s) giving the training;
 - The names of the staff who received training; and
 - The results of the tests undertaken by staff, where appropriate.
- (b) in relation to compliance monitoring –
- Reports by the compliance person to senior management; and
 - Records of consideration of those reports and of any action taken as a consequence.

Regulation 16(4)

- 8.20 An institution must establish and maintain systems which enable it to respond fully and rapidly to enquiries received from the Financial Intelligence Agency or law enforcement, relating to:
- Whether it maintains, or has maintained during the previous five years, a business relationship with any person; and
 - The nature of that relationship.

Form in which records have to be kept

- 8.21 Most institutions have standard procedures which they keep under review, and will seek to reduce the volume and density of records which have to be stored, whilst still complying with statutory requirements. Retention may therefore be:
- By way of original documents;
 - By way of photocopies of original documents;
 - On microfiche;
 - In scanned form; or
 - In computerized or electronic form.

- 8.22 The record retention requirements are the same, regardless of the format in which they are kept, or whether the transaction was undertaken by paper or electronic means.
- 8.23 Institutions involved in mergers, take-overs or internal reorganisations need to ensure that records of identity verification and transactions are readily retrievable for the required periods when rationalising computer systems and physical storage arrangements.

Location

- 8.24 The Regulations do not state where relevant records should be kept, but the overriding objective is for institutions to be able to retrieve relevant information without undue delay.
- 8.25 Where identification records are held in a country or territory other than Bermuda, it is the responsibility of the Bermuda entity to ensure that the records are available and do in fact meet Bermuda legal requirements. No secrecy or data protection legislation should restrict access to the records either by the Bermuda institution freely on request, or by Bermuda law enforcement agencies under court order. If it is found that such restrictions exist, copies of the underlying records of identity should, wherever possible, be sought and retained in Bermuda.
- 8.26 Institutions should take account of the scope of AML/ATF legislation in other countries, and should ensure that group records kept in other countries that are needed to comply with Bermuda legislation are retained for the required period.
- 8.27 Records relating to on-going investigations should be retained until the relevant law enforcement agency has notified the institution that the investigation has been closed. However, if an institution has not been advised of an on-going investigation within five years of the disclosure being made, the records may be dealt with in the normal course of the institution's records management policy.
- 8.28 When setting document retention policy, institutions must weigh the statutory requirements and the needs of the investigating authorities against normal commercial considerations. When original vouchers are used for account entry, and are not returned to the customer or his agent, it is of assistance to the law enforcement agencies if these original documents are kept to assist in forensic analysis. This can also provide evidence for institutions when conducting their own internal investigations.

APPENDIX I

GLOSSARY OF ABBREVIATIONS AND TERMS

AML/ATF	Anti-money laundering and anti-terrorist financing
ATFA	Anti-Terrorism (Financial and Other Measures) Act 2004
BMA	Bermuda Monetary Authority
CDD	Customer Due Diligence
CFATF	Caribbean Financial Action Task Force
EDD	Enhanced Due Diligence
FATF	Financial Action Task Force
FIA	Financial Intelligence Agency
IAIS	International Association of Insurance Supervisors
IMF	International Monetary Fund
IOSCO	International Organisation of Securities Commissions
KYC	Know Your Customer
PEP	Politically Exposed Person
POCA	Proceeds of Crime Act 1997
SAR	Suspicious Activity Report
SEA	Proceeds of Crime Regulations (Supervision and Enforcement) Act 2008
SDD	Simplified Due Diligence

AML/ATF Regulated Financial Institution – Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing) Regulations 2008 – Section 2(2)

AML/ATF regulated financial Institution means a person who —

- (a) carries on deposit-taking business within the meaning of section 4 of the Banks and Deposit Companies Act 1999;
- (b) carries on investment business within the meaning of section 3 of the Investment Business Act 2003;
- (c) is an insurer (and not a reinsurer) registered under section 4 of the Insurance Act 1978 who carries on long term business falling within paragraph (a) or (c) of the definition of “long-term business” in section 1(1) of the Insurance Act 1978;
- (d) is an insurance manager or broker registered under section 10 of the Insurance Act 1978 in so far as he acts as a manager or broker in connection with long term business (other than reinsurance business) falling within paragraph (a) or (c) of the definition of “long-term business” in section 1(1) of the Insurance Act 1978;
- (e) carries on the business of a fund administrator within the meaning of section 2(2) of the Investment Funds Act 2006;
- (f) carries on money service business within the meaning of section 20AA of the Bermuda Monetary Authority Act 1969;
- (g) carries on trust business within the meaning of section 9(3) of the Trusts (Regulation of Trust Business) Act 2001 and is not otherwise exempted by or under paragraph 3 of the Trusts (Regulation of Trust Business) Exemption Order 2002; or
- (h) is the operator of an investment fund within the meaning of section 2 of the Investment Funds Act 2006;

Basel CDD paper

Basel Committee Customer Due Diligence paper, published in October 2001.

Basel Consolidated KYC Risk Management Paper

Basel Committee paper on Consolidated KYC Risk Management, published in October 2004.

Basel Committee

The Basel Committee on Banking Supervision provides a forum for regular cooperation on banking supervisory matters and its objective is to enhance understanding of key supervisory issues and improve the quality of banking supervision worldwide. It seeks to do so by exchanging information on national

supervisory issues, approaches and techniques, with a view to promoting common understanding. At times, the Committee uses this common understanding to develop guidelines and supervisory standards in areas where they are considered desirable. The Committee encourages contacts and cooperation among its members and other banking supervisory authorities and it circulates to supervisors throughout the world both published and unpublished papers providing guidance on banking supervisory matters.

Beneficial owner(s) – Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing) Regulations 2008 - Regulation 3

(1) In the case of a **body corporate**, “beneficial owner” means any individual who—

- (a) as respects any body other than a company whose securities are listed on an appointed stock exchange, ultimately owns or controls (whether through direct or indirect ownership or control, including through bearer share holdings) more than 25% of the shares or voting rights in the body; or
- (b) as respects any body corporate, otherwise exercises control over the management of the body.

(2) In the case of a **partnership**, “beneficial owner” means any individual who—

- (a) ultimately is entitled to or controls (whether the entitlement or control is direct or indirect) more than a 25% share of the capital or profits of the partnership or more than 25% of the voting rights in the partnership; or
- (b) otherwise exercises control over the management of the partnership.

(3) In the case of a **trust**, “beneficial owner” means—

- (a) any individual who is entitled to a specified interest in at least 25% of the capital of the trust property;
- (b) as respects any trust other than one which is set up or operates entirely for the benefit of individuals falling within sub-paragraph (a), the class of persons in whose main interest the trust is set up or operates;
- (c) any individual who has control over the trust.

(4) In the case of a **legal entity or legal arrangement which does not fall within paragraph (1), (2) or (3)**, “beneficial owner” means

- (a) where the individuals who benefit from the entity or arrangement have been determined, any individual who benefits from at least 25% of the property of the entity or arrangement;
- (b) where the individuals who benefit from the entity or arrangement have yet to be determined, the class of persons in whose main interest the entity or arrangement is set up or operates;
- (c) any individual who exercises control over at least 25% of the property of the entity or arrangement.

(5) In the case of an **estate of a deceased person** in the course of administration, “beneficial owner” means the executor, original or by representation, or administrator for the time being of a deceased person.

(6) In **any other case**, “beneficial owner” means the individual who ultimately owns or controls the customer or on whose behalf a transaction is being conducted.

Compliance person

A person in an institution nominated by senior management to monitor the institution’s compliance with Bermuda’s anti-money laundering and anti-terrorist financing legislation, related regulations and guidance notes.

Criminal Conduct - Proceeds of Crime Act 1997 Section 3

Criminal Conduct means –

- (a) Drug trafficking, or
- (b) Any relevant offence.

Drug Trafficking Offence means an offence –

- (a) Under section 4, 5, 6(3), 7 or 11 of the Misuse of Drugs Act 1972 (importation, production, possession with intent to supply or handling of controlled drugs and cultivation of cannabis);
- (b) Under section 12 or 17 of the Criminal Justice (International Co-operation) (Bermuda) Act 1994 (manufacture and supply of scheduled substances and using ship for illicit traffic); or
- (c) Under section 43, 44 or 45 of this Act (money laundering) which relates to the proceeds of drug trafficking; or an offence under section 32, 33, 230 or 231 of the Criminal Code Act 1907 (attempt, incitement, conspiracy etc) deriving from such an offence.

Drug Trafficking means doing or being concerned in, whether in Bermuda or elsewhere, any act constituting –

- (a) A drug trafficking offence; or
- (b) An offence punishable under a corresponding law, and includes entering into or being otherwise concerned in, whether in Bermuda or elsewhere, a drug trafficking arrangement.

Drug Trafficking arrangement means an arrangement whereby –

- (a) The retention or control by or on behalf of another person of that other person's proceeds of drug trafficking is facilitated; or
- (b) The proceeds of drug trafficking by another person are used to secure that funds are placed at that other person's disposal or are used for that other person's benefit to acquire property by way of investment.

Relevant Offence means –

- (a) Any indictable offence in Bermuda other than a drug trafficking offence; or
- (b) Any act or omission which, had it occurred in Bermuda, would have constituted an indictable offence other than a drug trafficking offence.

Equivalent jurisdiction

A jurisdiction whose law contains equivalent provisions to those contained in the Proceeds of Crime Act 1997, the Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing) Regulations 2008 and the Anti-Terrorism (Financial and Other Measures) Act 2004 and the Anti-Terrorism (Financial and Other Measures) (Business in Regulated Sector) Order 2008..

FATF Recommendations

A series of Forty Recommendations on the structural, supervisory and operational procedures that countries should have in place to combat money laundering, issued by the Financial Action Task Force (FATF).

The Forty Recommendations were originally published in 1990, revised in 1996, and last revised in October 2004.

The FATF Forty Recommendations have been recognised by the International Monetary Fund and the World Bank as the international standards for combating money laundering.

These recommendations also apply to combating terrorist financing.

FATF Special Recommendations

FATF issued a series of Special Recommendations on Terrorist Financing in October 2001, and October 2004. The FATF Special Recommendations have been recognised by the International Monetary Fund and the World Bank as the international standards for combating the financing of terrorism.

International Association of Insurance Supervisors (IAIS) Guidance Paper 5

The International Association of Insurance Supervisors (IAIS) was established in 1994 and represents insurance regulators and supervisors of some 190 jurisdictions in nearly 140 countries, constituting 97% of the world's insurance premiums. IAIS published Guidance Paper No 5 in October 2004 providing guidance on anti-money laundering and combating the financing of terrorism.

Identification

Ascertaining the name of, and other relevant information about, a customer or beneficial owner.

International Organisation of Securities Commissions (IOSCO) Principles paper

IOSCO is recognized as the international standard setter for securities markets. The Organization's wide membership regulates more than 90% of the world's securities markets and IOSCO is the world's most important international cooperative forum for securities regulatory agencies. IOSCO members regulate more than one hundred jurisdictions and its membership is steadily growing. In 1998 IOSCO adopted a comprehensive set of Objectives and Principles of Securities Regulation (IOSCO Principles), which are today recognized as the international regulatory benchmarks for all securities markets. IOSCO published a paper entitled 'Principles on Client Identification and Beneficial Ownership for the Securities Industry' in May 2004.

Mind and management

Those individuals who, individually or collectively, exercise practical control over a non-personal entity.

Money Laundering – Proceeds of Crime Act 1997

An act which:

- Constitutes an offence under s.43, 44, 45;
- Constitutes an attempt, conspiracy or incitement to commit such an offence;
- Constitutes aiding, abetting, counselling or procuring the commission of such an offence; or
- Would constitute an offence specified above if done in Bermuda.

Money Laundering - Anti-Terrorism (Financial and Other Measures) Act 2004 S 8

A person commits an offence of money laundering if he enters into or becomes concerned in an arrangement which facilitates the retention or control by or on behalf of another person of terrorist property:

- By concealment;
- By removal from the jurisdiction;
- By transfer to nominees; or
- In any other way.

Occasional Transaction – Regulation 2(1)

Any transaction (carried out other than as part of a business relationship) amounting to \$15,000 or more, whether the transaction is carried out in a single operation or several operations which appear to be linked.

Politically Exposed Person – Regulation 11 & Schedule Paragraph 2

An individual who is or has, in a country or territory outside Bermuda, at any time in the preceding year, been entrusted with prominent public functions, an immediate family member, or a known close associate of a person who has been entrusted with such prominent public functions.

Reporting Officer

A person in an institution nominated by senior management to receive disclosures from others within the institution that have a knowledge or suspicion that a person is engaged in money laundering and where appropriate submit a suspicious activity report to the Financial Intelligence Agency.

Senior management

The directors and senior managers (or equivalent) of an institution who are responsible, either individually or collectively, for management and supervision of the institution's business.

Terrorist Financing

See sections 5 – 8 of the Anti-Terrorism (Financial and Other Measures Act 2004.

Terrorist Property – Anti-Terrorism (Financial and Other Measures) Act 2004 – S 4

- Money or other property which is likely to be used for the purposes of terrorism; or
- Proceeds of the commission of acts of terrorism; or
- Proceeds of acts carried out for the purposes of terrorism.

Tipping off – Proceeds of Crime Act 1997 S 47(1) & Anti-Terrorism (Financial and Other Measures) Act 2004 S 10A(1)

A tipping-off offence is committed if a person knows or suspects that the police are acting or proposing to act in connection with an investigation which is being, or is about to be conducted into money laundering or terrorist financing and he discloses to any other person information or any other matter which is likely to prejudice that investigation or proposed investigation.

Tipping off – Proceeds of Crime Act 1997 S 47(2) & Anti-Terrorism (Financial and Other Measures) Act 2004 S 10A(2)

A tipping-off offence is committed if a person knows or suspects that a disclosure has been made to the Financial Intelligence Agency or an appropriate person and he discloses to any other person information or any other matter which is likely to prejudice any investigation which might be conducted following such a disclosure.

Transparency International Corruption Perceptions Index

[2008/cpi/surveys_indices/policy_research](http://www.transparency.org/cpi/surveys_indices/policy_research)

Annually Transparency International produces a “Corruption Perceptions Index”, which ranks approximately 150 countries according to their perceived level of corruption.

Verification

Verifying the identity of a customer, by reference to reliable, independent source documents, data or information, or of a beneficial owner through carrying out risk-based and adequate measures.

Wolfsberg Group

An association of twelve global banks, which aims to develop financial services industry standards, and related products, for Know Your Customer, Anti-Money Laundering and Counter Terrorist Financing policies.

Wolfsberg Principles

These are contained in four documents:

- Global Anti-Money Laundering Guidelines for Private Banking, published by the Wolfsberg Group in October 2000, and revised in May 2002;
- Statement on the Suppression of the Financing of Terrorism, published in January 2002;
- Anti-Money Laundering Principles for Correspondent Banking, published in November 2002; and
- Statement on Monitoring, Screening and Searching, published in September 2003.

APPENDIX II

ANTI-MONEY LAUNDERING & ANTI-TERRORIST FINANCING RESPONSIBILITIES IN BERMUDA

Bermuda Monetary Authority

Bermuda's financial regulator - objectives and responsibilities include:

- Monitoring AML/ATF regulated financial institutions to ensure full compliance with Bermuda's AML/ATF framework;
- Assisting with the detection and prevention of financial crime;
- Deterring and disrupting criminal and terrorist activity by increasing the risk and lowering the reward faced by perpetrators; and
- Issuing Guidance to AML/ATF regulated financial institutions supervised for compliance with the AML/ATF regulations.

Bermuda Police Service

Investigative body responsible for investigating all criminal activity in Bermuda, which includes money laundering, acts of terrorism and terrorist financing.

Financial Intelligence Agency:

Bermuda's financial intelligence agency receives reports concerning suspicions of money laundering and terrorist financing. The Financial Intelligence Agency collates, analyses and if appropriate, disseminates reports to law enforcement for investigation.

HM Customs

Responsible for:

- Interdicting illicit drugs and contraband.
- Monitoring the movement of passengers and cargo.
- Monitoring cash declarations on export or import.
- Monitoring the cross border movements of currency and bearer negotiable instruments.
- Enforcing compliance with Bermuda's Customs laws and regulations.

National Anti-Money Laundering Committee

Established under S 49 of the Proceeds of Crime Act 1997 for the purpose of –

(a) advising the Minister in relation to the detection and prevention of money laundering, and on the development of a national plan of action to include recommendations on effective mechanisms to enable the competent authorities in Bermuda to coordinate with each other concerning the development and implementation of policies and activities to combat money laundering, and;

(b) advising the Minister as to the participation of Bermuda in the international effort against money laundering.

The Chairman of the Committee is appointed by the Minister of Justice and must be a person with relevant experience. The Committee meet on a regular basis to carry out its duties and the members are –

- The Chairman;
- The Solicitor General;
- The Financial Secretary;
- The Permanent Secretary of the Ministry responsible for the Police;
- The Commissioner of Police;
- The Director of the FIA;
- The Chief Executive Officer of the Bermuda Monetary Authority;
- The Director of Public Prosecutions;
- The Permanent Secretary Ministry of Justice;

- The Collector of Customs; and
- Such other persons as the Minister may from time to time appoint.

Office of the Director Public Prosecutions

Prosecutes all crimes, including money laundering and terrorist financing in Bermuda.

APPENDIX III

BERMUDA LEGISLATION & GUIDANCE

Bermuda legislation is available at www.bermulaweb.com

- Proceeds of Crime Act 1997.
- Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing) Regulations 2008.
- Financial Intelligence Agency Act 2007.
- Anti-Terrorism (Financial and Other Measures) Act 2004.
- Anti-Terrorism (Financial and Other Measures) (Business in Regulated Sector) Order 2008.
- Proceeds of Crime (Designated Countries and Territories) Order 1998.
- The Criminal Justice (International Cooperation) (Bermuda) Act 1994.
- Revenue Act 1898.
- The Terrorism (United Nations Measures) (Overseas Territories) Order 2001.
- The Al-Qa'ida and Taliban (United Nations Measures) (Overseas Territories) Order 2002.
- The Al-Qa'ida and Taliban (United Nations Measures) (Overseas Territories) (Amendment) Order 2002.
- Bermuda Monetary Authority Act 1969.
- Proceeds of Crime (Supervision and Enforcement) Act 2008.
- Guidance Notes for AML/ATF regulated financial institutions on Anti-Money Laundering and Anti-Terrorist Financing.

Proceeds of Crime Act 1997

The Proceeds of Crime Act 1997 establishes the offence of money laundering and creates penalties for committing such offences, gives investigative powers to the police and provides for the tracing and confiscation of the proceeds of criminal conduct.

- Creates investigative powers for the law enforcement agencies:
 - Production orders;
 - Search warrants;
 - Monitoring orders;
 - Customer information orders; and
 - Disclosure of information by Government departments orders.
- Establishes the following criminal offences:
 - To acquire, use, possess, conceal, disguise, convert, transfer or remove the proceeds of criminal conduct from the jurisdiction;
 - To enter into or become concerned in an arrangement whereby retention or control of another persons proceeds of criminal conduct is facilitated;
 - The proceeds of criminal conduct are used to secure funds or are used to acquire property by way of investment;
 - For any person to fail to make a report where they have knowledge or suspicion of money laundering, as soon as is reasonably practicable after the information came to their attention in the course of their trade, profession, business or employment;
 - For anyone to disclose information likely to prejudice an investigation by i.e. “tipping off” or disclosing information regarding the filing of a suspicious activity report; and
 - For an institution to fail to comply with a requirement imposed on it under a customer information order, or in knowingly or recklessly making a statement in purported compliance with a customer information order that is false or misleading in a material particular.

Note: An offence is not committed if a person reports his knowledge or suspicion to the Financial Intelligence Agency or under approved internal arrangements, either before the prohibited act is carried out, or as soon afterwards as is reasonably practicable.

- Sets out maximum penalties:
 - For the offence of money laundering of 20 years imprisonment and/or an unlimited fine.
 - For failing to make a report of suspected money laundering, or for “tipping off” or disclosing information knowing that a suspicious activity report has been made, of ten years’ imprisonment and/or an unlimited fine.

Anti-Terrorism (Financial and Other Measures) Act 2004

The Anti-Terrorism (Financial and Other Measures) Act 2004 establishes a series of offences related to involvement in arrangements for facilitating, raising or using funds for terrorism purposes and gives investigative powers to the police. The Act:

- Creates investigative powers for the law enforcement agencies:
 - Production orders;
 - Search warrants; and
 - Monitoring orders.
- Establishes the following criminal offences:
 - To invite another to provide money or other property intending that it should be used or suspecting that it may be used for the purposes of terrorism;
 - To receive money or other property intending that it should be used or suspecting that it may be used for the purpose of terrorism;
 - To provide money or other property knowing or suspecting that it will or may be used for the purpose of terrorism;
 - To use money or other property for the purposes of terrorism;
 - To possess money or other property intending that it should be used or suspecting that it may be used for the purposes of terrorism;
 - To enter into or become concerned in arrangement as a result of which money or other property is made available or is to be made available to another knowing or suspecting that it will or may be used for the purposes of terrorism;
 - To enter into or become concerned in arrangement which facilitates the retention or control by or on behalf of another person of terrorist property by concealment, removal from the jurisdiction, by transfer to nominees or in any other way; and
 - To not report a belief or suspicion that another person has committed an offence of involvement in arrangements for facilitating, raising or using funds for terrorism purposes.
- Sets out the following penalties:
 - The maximum penalty for failure to report is five years’ imprisonment, and/or a \$100,000 fine; and
 - The maximum penalty for the offence of actual money laundering is 14 years imprisonment, and/or a \$200,000 fine.

The Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing) Regulations 2008

The Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing) Regulations 2008 specify arrangements which must be in place in institutions within the scope of the Regulations, in order to prevent operations relating to money laundering or terrorist financing.

The Regulations apply to all AML/ATF regulated financial institutions as defined at section 2(2):

Institutions within the scope of the Regulations are required to establish adequate and appropriate policies and procedures in order to prevent operations relating to money laundering or terrorist financing, covering:

- Customer due diligence;
- Internal and external reporting;

- Record-keeping;
- Internal control;
- Risk assessment and management;
- Compliance management; and
- Communication.

Whether a breach of the Regulations has occurred is not dependent on whether money laundering or terrorist financing has taken place: institutions are liable to civil penalties for not having adequate AML/ATF systems in place - failure to comply with any of the requirements of the Regulations may expose the institution to such penalties.

Proceeds of Crime Regulations (Supervision and Enforcement) Act 2008

The BMA is the supervisory authority for AML/ATF regulated financial institutions and has a duty to effectively monitor relevant persons that it supervises, and take necessary measures for the purpose of securing compliance with the Regulations. The BMA has enforcement powers and can impose civil penalties on institutions that it determines has failed to comply with the Regulations.

The Financial Intelligence Agency Act 2007

The Financial Intelligence Agency Act establishes an independent agency to receive reports of suspicious transactions from institutions and other persons and to collate, analyse and if appropriate disseminate to law enforcement for investigation.

The Terrorism (United Nations Measures) (Overseas Territories) Order 2001

Gives effect to UNSCR 1373 and prohibits fund raising for terrorism purposes and restricts the making available of funds and financial services to terrorist organisations and providing powers to freeze accounts of suspected terrorist organisations. The Order requires relevant institutions, to report to the Governor if they become aware, or suspect that a customer has been involved in the commission of offences under the Resolution or is controlled or owned by a person who has committed such offences.

The Al-Qa'ida and Taliban (United Nations Measures) (Overseas Territories) Order 2002

Gives effect to UNSCR 1390 and prohibits the making of funds available, the delivery or supply of arms and related material, technical assistance or training to listed persons. The Order also contains powers for the Governor to issue a Notice freezing funds if there are reasonable grounds for suspecting that the holder may be a listed person or holding funds on behalf of a listed person. The Order requires relevant institutions, to notify the Governor if the institution becomes aware, or suspects, a customer is a listed person or has committed an offence specified in the Order.

The Al-Qa'ida and Taliban (United Nations Measures) (Overseas Territories) (Amendment) Order 2002

Amends the Al-Qa'ida and Taliban (United Nations Measures) (Overseas Territories) Order 2002. The definition of relevant institution is amended, however deposit taking institutions remain affected by the Order.